NETGEAR

NETGEAR ProSafe VPN Client

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

April 2012
202-10684-04
v1.0

©2010–2012 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

For GNU General Public License (GPL) related information, please visit
http://support.netgear.com/app/answers/detail/a_id/2649

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at
http://support.netgear.com/app/answers/detail/a_id/984

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. ©2010–2012 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10684-04	v1.0	March 2012	Minor new features and improvements such as the Remote Sharing pane.
202-10684-03	v1.0	May 30, 2011	Major revision to document the new format of the user interface and some new features such as the enhanced capability to change languages.
202-10684-02	v1.1	December 2010	Minor editorial changes and addition of an index.
202-10684-02	v1.0	December 2010	Reorganization and revision of the entire manual.
202-10684-01	v1.0	June 2010	First publication.

Contents

Chapter 1 Introduction

Linux Appliance Support 7
VPN Client Features 8
VPN Client Licenses 10

Chapter 2 Installation

Software Installation 12
Trial Software Evaluation 13
Software Activation 15
Software Activation Wizard 15
Troubleshooting Activation 17
Software Upgrade 19
Software Uninstallation 20

Chapter 3 User Interface Overview

User Interface Elements 21
System Tray Popup Screens 23
Keyboard Shortcuts 24
Connection Panel Screen 24
Configuration Panel Screen 25
Main Menu 26
Status Bar 26
About Screen 26
Options Screen 27
Wizards 32
VPN Console Active Screen 33

Chapter 4 Basic Tasks

Open a VPN Tunnel 34
Easily Import a VPN Configuration 35
Specify a Certificate for User Authentication 35
Open a VPN Tunnel before Windows Logon 37

Chapter 5 Connection Panel Screen Tasks

Chapter 6 Configuration Panel Screen Tasks

Use the Configuration Wizard to Create a VPN Tunnel Connection 41

Manually Create a VPN Tunnel Connection 44
Authentication or Phase 1 45
Configure Authentication 45
Configure Advanced Authentication 47
IPSec or Phase 2 52
Configure IPSec 52
Advanced IPSec Configuration 55
Script Configuration 57
Remote Sharing 59
Global Parameters 60
USB Mode 62
Enable a New USB Drive with a VPN Configuration 62
Automatic Opening of Tunnels 66
Certificate Management 66
Assign Certificates 67
View Certificate Details 68
Import Certificates 69
Use Certificates from USB Tokens and Smart Cards 73
Certificate Troubleshooting 74
VPN Configuration Management 76
Import or Export a VPN Configuration 76
Merge VPN Configurations 78
Split a VPN Configuration 78
Embed Your Own VPN Configuration in a VPN Client Software Setup . 80
Demo VPN Configuration 80

Chapter 7 VPN Client Software Setup and Deployment

Embedded VPN Configuration 81
VPN Client Software Setup Commands 82
Software Setup for GUI Mode 83
Software Setup for GUI Mode with Access Control 83
Software Setup for System Tray Menu Items 84
Other Software Setup Options 85
Command-Line Interface Commands 87
Open or Close VPN Tunnels 87
Stop the VPN Client 88
Import, Export, Add, or Replace the VPN Configuration 88
Support for ATR Codes (Using Smart Cards) 89

Chapter 8 Configure the VPN Client with a NETGEAR Router

Introduction 91
Sample VPN Network Topology 92
Configure the SRX5308 VPN Router 93
Use the VPN Wizard to Configure a Client-to-Router VPN Connection . 93
Manually Configure a Client-to-Router VPN Connection 99
Configure the VPN Client 103
Use the Configuration Wizard to Configure the VPN Client 103

Manually Configure the VPN Client 108
Establish a VPN connection 114

Chapter 9 VPN Troubleshooting

Overview. 116
Resolving Firewall Interference 117
Typical Errors 117
“PAYLOAD MALFORMED” Error (Wrong Phase 1 [SA]) 117
“INVALID COOKIE” Error 117
“no keystate” Error 118
”received remote ID other than expected” Error 118
“NO PROPOSAL CHOSEN” Error (Phase 1) 119
“NO PROPOSAL CHOSEN” Error (Phase 2) 119
“INVALID ID INFORMATION” Error 119
Other Common Problems. 120
There Is No Response to a Phase 1 Request 120
The Console Shows Only “SEND” and “RECV” 121
There Is No Response to a Phase 2 Requests 121
A Tunnel No Longer Opens 121
A VPN Tunnel Is Up but You Cannot Ping the Remote Endpoint. 121
View the Logs 122

Appendix A VPN Client Software Setup Deployment and Command-Line Interface Guide

Overview. 125
VPN Client Software Setup Deployment 126
Silent Installation. 126
Create a Silent VPN Client Software Setup 126
Deploy a VPN Client Software Setup from a CD-ROM 127
Run a VPN Client Software Setup from a Shortcut (Double-Click an Icon) 128
Deploy a VPN Client Software Setup Using a Batch Script 128
Deploy a VPN Client Software Setup from a Network Drive. 129
Deploy a VPN Client Software Update 130
Customize VPN Client Software for End Users 130
Limit Usage of the VPN Client to the Connection Panel. 130
Specify Display of the Connection Panel Screen in a VPN Client Software Setup 131
Limit Usage to the Connection Panel Screen in a VPN Client Software Setup 131
Limit Usage of the VPN Client to the System Tray Icon Menu in a VPN Client Software Setup 132
VPN Configuration Deployment 132
Embed a VPN Configuration in the VPN Client Software Setup. 132
Export and Deploy a New VPN Configuration 133
VPN Automations 133
Create a Batch or Script That Automatically Opens or Closes a

Tunnel. 133
Automatically Open a Web Page When a VPN Tunnel Opens 134
Open a Tunnel with a Double-Click on a Desktop Icon 134
Software Setup Command Reference 135
Command-Line Interface Command Reference. 139

Appendix B Generating Certificates With Microsoft Certificates Services and OpenSSL

Microsoft Certificates Services 143
Install Microsoft Certificate Services. 143
Generate a User Certificate with Microsoft Certificate Services. 147
Sign a Certificate Request 149
Export Certificates 150
OpenSSL 152
Generate a Certificate with OpenSSL 153
Displaying Certificate Information Using TgbSmallPKI Tools. 156

Appendix C References and Useful Websites

Index

Introduction

1

The VPN Client supports all Windows versions and allows you to establish secure connections over the Internet usually between a remote worker and the corporate Intranet. IPSec is the most secure way to connect to the enterprise as it provides strong user authentication and strong tunnel encryption with the ability to work with existing network and firewall settings.

This chapter includes the following sections:

- *Linux Appliance Support*
- *VPN Client Features*
- *VPN Client Licenses*

> ***Note:*** For more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

Linux Appliance Support

The VPN Client supports several versions of Linux IPSec VPN such as StrongS/WAN and FreeS/WAN. The VPN Client is compatible with most of the IPSec routers and appliances that are based on those Linux implementations.

VPN Client Features

The VPN Client has the following features.

Table 1. List of features

Feature	Specifications
Windows versions	• Windows 2000 32-bit • Windows XP 32-bit • Windows Server 2003 32-bit • Windows Server 2008 32/64-bit • Windows Vista 32/64-bit • Windows 7 32/64-bit
Languages	Arabic, Chinese (simplified), Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hindi, Hungarian, Italian, Japanese, Norwegian Polish, Portuguese, Russian, Serbian, Slovenian, Spanish, Thai, and Turkish.
Connection modes	• Operates in a peer-to-peer VPN mode as well as point-to-multiple mode without a gateway or server. All connection types such as dial-up, DSL, cable, GSM/GPRS, and Wi-Fi are supported. • Allows IP range networking. • Runs in a Remote Desktop Protocol (RDP) connection session.
Tunneling protocols	• Full Internet Key Exchange (IKE) support: the IKE implementation is based on the OpenBSD 3.1 implementation (ISAKMPD). This provides the best compatibility with existing IPSec routers and gateways. • Full IPSec support: - Main mode and aggressive mode - MD5, SHA-1, and SHA-256 hash algorithms - Change IKE port
NAT Traversal	• NAT Traversal Draft 1 (enhanced), Draft 2, and Draft 3 (full implementation), including: - NAT OA support - NAT keep-alive - NAT-T aggressive mode • Forced NAT-Traversal mode
SIP/VoIP support	Support for Session Initiation Protocol (SIP) and Voice over IP (VoIP) traffic in a VPN tunnel (Window Vista and WIndows 7 only).
Encryption	Provides the following encryption algorithms: • 3DES, DES, and AES 128/192/256-bit encryption • Support for Diffie-Hellman group 1 (768 bits), group 2 (1024 bits), group 5 (1536 bits), and group 14 (2048 bits)

Table 1. List of features (continued)

Feature	Specifications
User authentication	Supports the following user authentication methods: • Preshared keying and X509 certificate support. Compatible with most of the currently available IPSec gateways. • Extended authentication (AUTH). • Flexible certificates: PEM, PKCS#12 certificates can be directly imported from the user interface. Ability to configure one certificate per tunnel. • Hybrid authentication method.
	Certificate storage capabilities: • USB token and smart card support • Personal Certificate Store support • VPN configuration file
	Remote login: Vista Credential Providers support (also known as GIna on Windows 2000 and Windows XP) to enable Windows logon using a VPN tunnel or choose to log on to a local machine.
Dead Peer Detection	Dead Peer Detection (DPD) is an IKE extension (RFC3706) for detecting a dead IKE peer.
Redundant Gateway	The Redundant Gateway feature provides a highly reliable secure connection to a corporate network. The Redundant Gateway feature allows the VPN Client to open an IPSec tunnel with an alternate gateway if the primary gateway is down or not responding.
Mode Config	Mode Config is an IKE extension that enables the VPN gateway to provide LAN configuration to the remote user's machine (that is, the VPN Client). With Mode Config, you can access all servers on the remote network by using their network name (for example, \\myserver\marketing\budget) instead of their IP address.
USB drive	You can save VPN configurations and security elements (certificates, preshared key, and so on) to a USB drive to remove security information (for example, user authentication) from the computer. You can automatically open and close tunnels when plugging in or removing the USB drive. You can attach a VPN configuration to a specific computer or to a specific USB drive.
Smart card and USB token	The VPN Client can read certificates from smart cards to make full use of existing corporate ID or employee cards that carry digital credentials. You can easily import smart card ATR codes to enable new smart card and USB token models that are not yet in the software.
Log console	All phase messages are logged for testing or staging purposes.
Flexible user interface	• Silent install and invisible graphical interface allow network administrators to deploy solutions while preventing user misuse of configurations. • Small Connection Panel screen and VPN Configuration Panel screen can be available to end users separately with access control. • Drag and drop VPN configurations into the VPN Client. • Keyboard shortcuts to easily navigate the VPN Client.

Table 1. List of features (continued)

Feature	Specifications
Scripts	Scripts or applications can be launched automatically on events (for example, before and after a tunnel opens, or before and after a tunnel is closed).
Configuration management	• User interface and command-line interface (CLI). • Password-protected VPN configuration file. • Specific VPN configuration file can be provided within the setup. • Embedded demo VPN configuration to test and debug with online servers. • Ability to prevent software upgrade or uninstallation if protected by password.
Live update	Ability to check for online updates.

VPN Client Licenses

NETGEAR products can include a license for the VPN Client Lite or for a 30-day trial copy of the VPN Client Professional, or for both. The following table lists the features that are included in the VPN Client Lite and VPN Client Professional versions. When you launch the VPN Client, you are given the opportunity to purchase a license for the Professional VPN Client and to activate (register) either the VPN Client Professional or VPN Client Lite.

The following table compares the features of the VPN Client Professional and VPN Client Lite.

Table 2. Feature comparison between VPN Client Lite and VPN Client Professional

VPN Client Functions		Lite	Pro
Configuration	Configuration wizard	✓	✓
	X-Auth	✓	✓
	Mode Config	✓	✓
	DNS/WINS server manual configuration	✓	✓
	Hybrid mode		✓
	IKE/NAT-T ports can be modified		✓

Table 2. Feature comparison between VPN Client Lite and VPN Client Professional (continued)

VPN Client Functions		Lite	Pro
Control	Connection panel	✓	✓
	Console logs	✓	✓
	Disable split tunneling	✓	✓
	Dead Peer Detection	✓	✓
	System tray popup	✓	✓
	GUI protection (password)		✓
	Auto Open (Windows on startup on traffic detection)		✓
	Start VPN tunnel before Windows logon		✓
	Easy deployment by command-line interface (CLI)		✓
Advanced Features	Multitunnel configurations		✓
	Redundant Gateways	✓	✓
	Scripts		✓
	USB mode		✓

2 Installation

This chapter describes installation of the VPN Client and related processes. This chapter includes the following sections:

- *Software Installation*
- *Trial Software Evaluation*
- *Software Activation*
- *Software Upgrade*
- *Software Uninstallation*

Software Installation

The VPN Client software installation does not require specific information and is self-explanatory. After completing the installation, you are asked to reboot your computer. However, if your operating system is Windows 7 or Windows Vista, you can install the VPN Client software without rebooting your computer.

After you have rebooted and logged in to your computer, the VPN Client Activation Wizard screen displays. The information about how to proceed depends on whether you want to use a trial license or activate a permanent license:

- If you downloaded a free trial software version, see *Trial Software Evaluation* on page 13.
- If you purchased a permanent license, see *Software Activation* on page 15.

➢ **To launch the VPN Client after software installation, use one of the following three methods:**

- On your desktop, double-click the VPN Client shortcut.
- In the taskbar, click the VPN Client icon.
- From the Start menu, select the path to the VPN Client, for example, **Start > Programs > Netgear > NETGEAR VPN Client**.

Note: *If your operating system is Windows 7 or Windows Vista, you can select a check box to automatically run the VPN Client after software installation.*

Note that the VPN Client creates new rules in the Windows firewall (Vista and later operating systems) so that VPN traffic is enabled: UDP ports 500 and 4500 are authorized both for authentication (phase 1) traffic and for IPSec (phase 2) traffic.

If you use an earlier Windows operating system or another firewall, you might have to create firewall rules to enable the VPN Client. For information, see *Resolving Firewall Interference* on page 117.

Trial Software Evaluation

The following figure shows the Software Activation screen while the evaluation period is active.

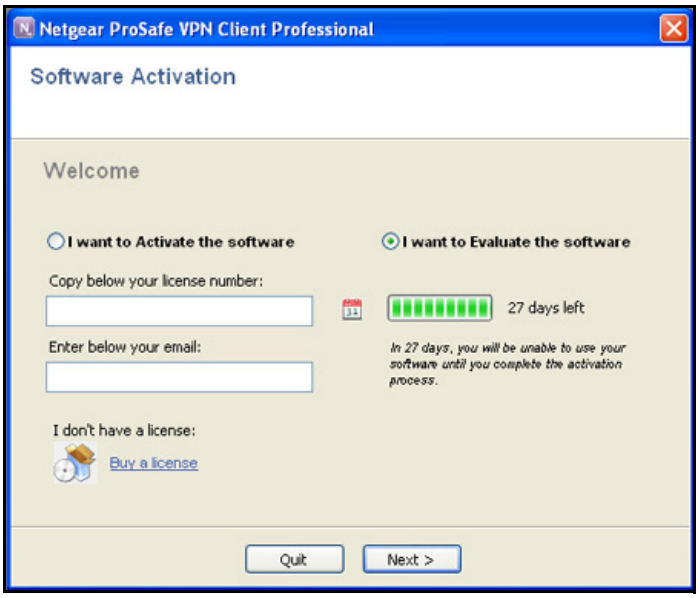


Figure 1.

➢ **To use the VPN Client during the evaluation period (usually limited to 30 days):**

1. Select the **I want to evaluate the software** radio button. You do not need to enter a license number and email address to activate the trial software.
2. Click **Next**.

During the evaluation period, the Software Activation screen displays each time that you start the VPN Client. The remaining days of the evaluation period is displayed next to the calendar icon on the right of the screen.

When the evaluation period expires, the following occurs:

- The **I want to Activate the software radio** button is automatically selected.
- The **I want to Evaluate the software** radio button is masked out.
- The message *Evaluation period expired* is displayed.
- The software is disabled.

In order for you to use the VPN Client, you need to purchase and activate a permanent license. You can click the **Buy a license** link to purchase a permanent license.

The following figure show the Software Activation screen after the evaluation period has expired:

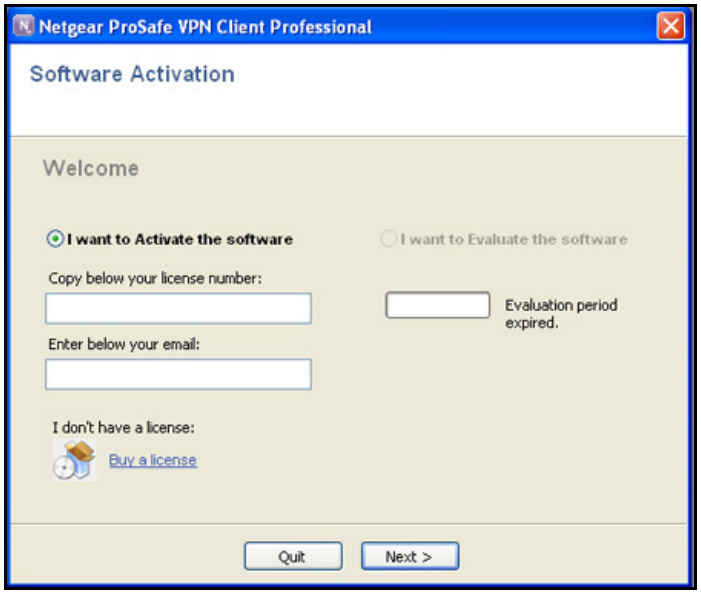


Figure 2.

During the evaluation period, the Software Activation screen is accessible by selecting **? > Activation Wizard** from the main menu on the Configuration Panel screen (see *Software Activation* on page 15). You can purchase and activate a permanent license while you are still in the evaluation period or after the evaluation period has expired.

You can see the remaining time of the evaluation period on the About screen by selecting **? > About** from the main menu of the Connection Panel screen.

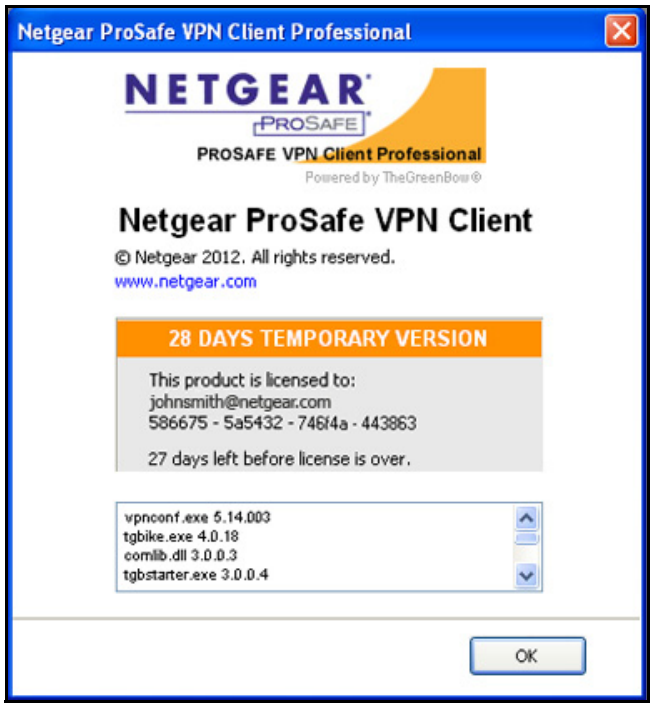


Figure 3.

Software Activation

When you purchase a permanent license, you are required to activate it before you can use the VPN Client.

Software Activation Wizard

In order for you to use the VPN Client beyond the evaluation period, the VPN Client license need to be activated on your computer. You need the license number or key and an email address.

To transfer a license to a new computer, you need to uninstall the software from the old computer. Deactivation of the license on the old computer occurs automatically if the computer is connected to the Internet. The license can then be used to activate the VPN Client on a new computer.

➢ **To activate your software using the Activation Wizard:**

1. Make sure you are connected to the Internet.
2. Launch the Activation Wizard from the VPN Client by selecting **? > Activation Wizard** from the main menu on the Configuration Panel screen. The following figure shows a situation in which the evaluation period has not yet expired.

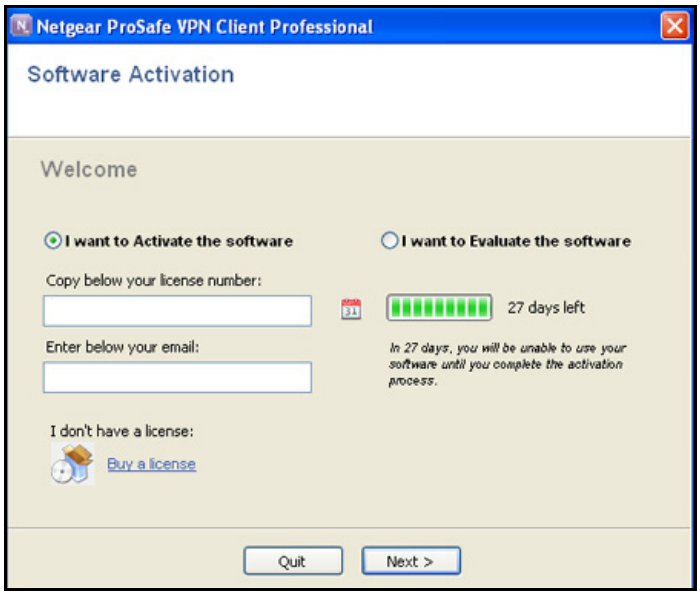


Figure 4.

3. Select the **I want to Activate the software** radio button.
4. Enter your permanent license number.
5. Enter your email address, which will be used to send you the activation confirmation.

> ***Note:*** The email address might not be required. If the network administrator suppresses display of the Email address field during the software setup, it will not be displayed by the Software Activation Wizard. Suppression can be used to centralize all software activation confirmation emails to a single email address.

6. Click **Next**. The Activation Wizard attempts to automatically connect to the activation server to activate the VPN Client software. The progress bar shows the activation progress. When the activation is complete, the screen shows whether or not the activation was successful and displays messages associated with the outcome (see also *Troubleshooting Activation* on page 17).

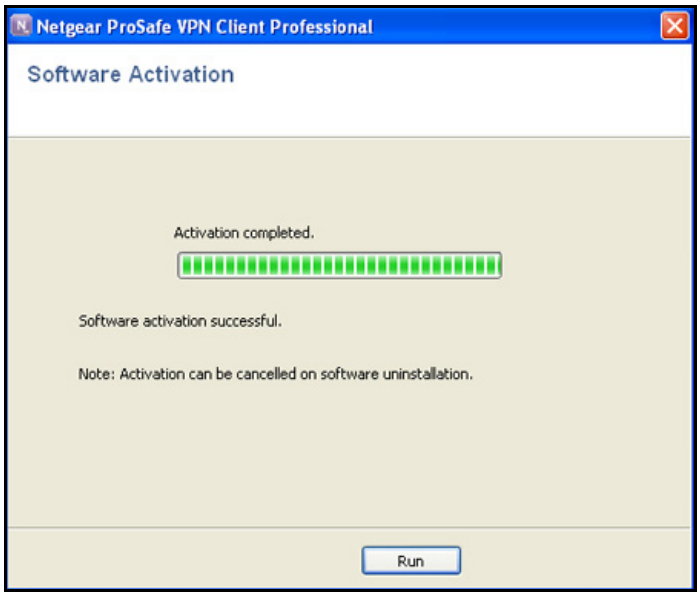


Figure 5.

7. Click **Run** to open the VPN Client with the new license.

Tip: After activation, save the license key number. You might need it again to reactivate your software in case of a problem. Also, keep the CD label for technical support.

Note: You can change the license number at any time, but you first need to uninstall the VPN Client.

Note: A license number is attached to a single computer after activation. However, you can deactivate the license number and transfer it to another computer.

Troubleshooting Activation

Errors can occur during the activation process. Each activation error type is displayed on the Software Activation screen. Click the **More information about this error** link at the bottom of the screen for information about the error and recommendations. The following two figures show examples of activation errors.

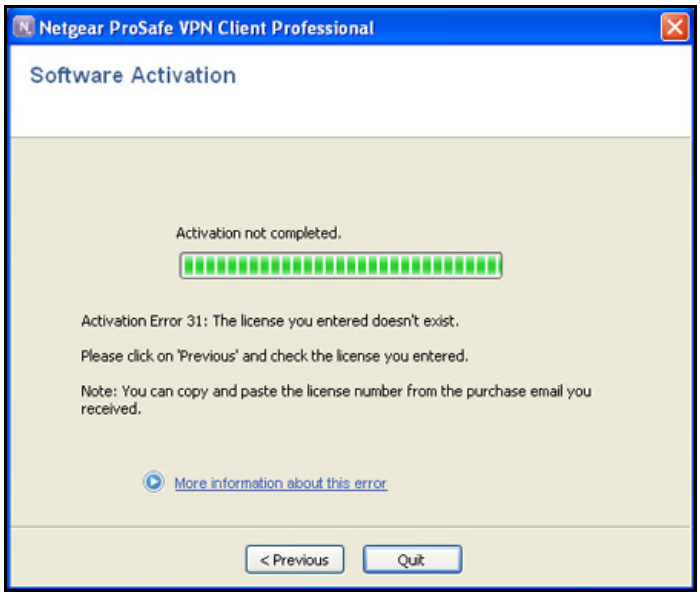


Figure 6.

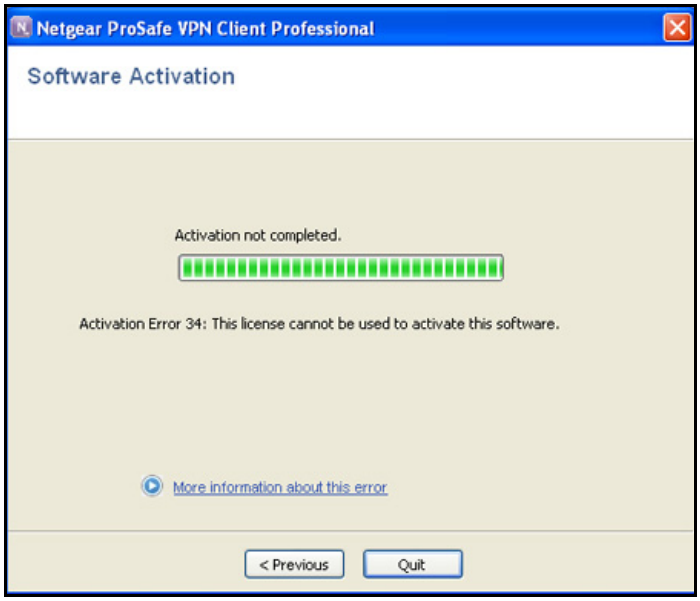


Figure 7.

You can resolve most of errors by carefully checking the following:

- Verify that you entered the correct license number. (Error 031 indicates that the license number was not found.)
- Your license number could already be activated (Error 033). Contact NETGEAR support.
- Your license number cannot be used for activation (Error 034). Contact NETGEAR support.

- Communication with the activation server might be blocked by a firewall (error 053 or error 054). Find out if a personal or corporate firewall is blocking communications.
- The activation server might be temporarily unreachable. Wait a few minutes and try again.

All activation errors are listed at *www.netgear.com/support*.

Software Upgrade

> ***Note:*** The VPN Client must be activated after each software upgrade. Depending on your maintenance contract, a software upgrade activation might be rejected. Carefully read the recommendations in this section and check the current status of your software release by selecting **? > Check for Update** from the main menu of the Connection Panel screen.

The success of a software upgrade activation depends on your maintenance contract:

- During the maintenance period (which starts from your first activation), all software upgrades are allowed.
- If the maintenance period has expired or if you have no maintenance contract, only maintenance software upgrades are allowed. Maintenance software upgrades are identified by the last digit of a version.

  Example: Your maintenance period has expired and your current software release is 3.12. You can upgrade to releases 3.13 through 3.19 but not to release 3.20, 3.30, 4.00, or 5.00.

If you want to subscribe or extend your maintenance period, please contact NETGEAR by email at *sales@netgear.com*.

> ***Note:*** The VPN configuration is saved during a software upgrade and automatically reenabled within the new release.

> ***Note:*** If you have specified a password in the access control Configuration screen (see *View Pane: Access Control and Hidden Interface* on page 27), you need to enter it to be able to upgrade the software.

Software Uninstallation

If you need to, you can uninstall the VPN Client.

➢ **To uninstall the VPN Client, use one of the following two methods:**

- Open the Windows Control Panel, double-click **Add or Remove Programs**, select **NETGEAR VPN Client**, and then select **Remove**.
- From the Start menu, select the path to the VPN Client, for example, **Start > Programs > Netgear > NETGEAR VPN Client**, and then the uninstall option.

When you uninstall the VPN Client, make sure that your computer is connected to the Internet. If your computer is not connected to the Internet, contact NETGEAR support by email at *support@netgear.com* or call the technical center to inactivate your license key.

Tip: After uninstallation, save the license key number. You might need it again to reactivate your software. Also, keep the CD label for technical support.

User Interface Overview

3

This chapter describes the user interface for the VPN Client. This chapter includes the following sections:

- *User Interface Elements*
- *System Tray Popup Screens*
- *Keyboard Shortcuts*
- *Connection Panel Screen*
- *Configuration Panel Screen*
- *VPN Console Active Screen*

User Interface Elements

The VPN Client is fully autonomous and can start and stop tunnels without user intervention, depending on traffic to certain destinations. However, it requires a VPN configuration.

The VPN Client configuration is defined in a VPN configuration file. The software user interface allows creating, modifying, saving, exporting, or importing the VPN configurations together with security elements such as a preshared key or certificates.

The user interface consists of several elements:

- Configuration Panel
- Connection Panel
- Main menus
- System tray icon and popup screens
- Status bar
- Wizards
- Preferences

You can launch the VPN Client by double-clicking the application icon on the desktop or Windows Start menu or by single-clicking the application icon in the system tray. Once launched, the VPN Client displays an icon in the system tray that indicates whether or not a tunnel is opened, using a color code.

Green icon:
at least one VPN tunnel opened.

Purple icon:
no VPN tunnel opened.

Figure 8.

Right-click the VPN Client icon in the system tray to open the system tray menu.

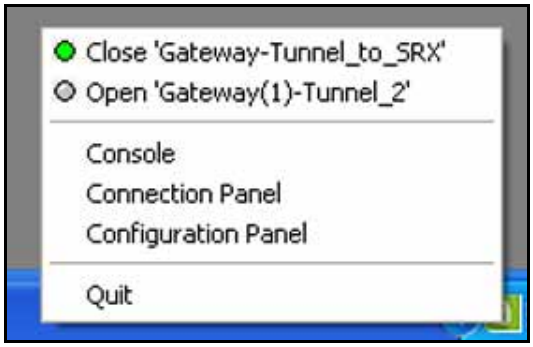


Figure 9.

The system tray menu shows the following items from top to bottom:

- Configured tunnels with their current status. You can open or close tunnels by selecting **Open '*<gateway name-tunnel name>*'** or **Close '*<gateway name-tunnel name>*'**.
- **Console**. Shows the VPN Console Active screen.
- **Connection Panel**. Opens the Connection Panel screen, which lets you open and close VPN tunnels and displays information about VPN tunnels.
- **Configuration Panel**. Opens the Configuration Panel screen, which lets you create and configure VPN tunnels.
- **Quit**. Closes all established VPN tunnels, then closes the VPN Client.

System Tray Popup Screens

When a VPN tunnel opens or closes, a small popup screen comes out from the system tray icon and shows the following:

- VPN tunnel opening with different phases. The popup screen disappears after 6 seconds unless you move the mouse over the screen.

Figure 10.

- VPN tunnel closing, followed by tunnel closed.

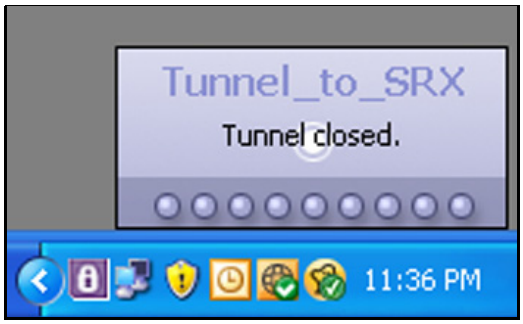


Figure 11.

- If the VPN tunnel cannot open, the screen might display a warning with a link to more information.

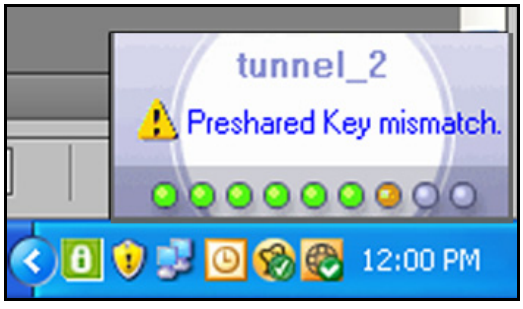


Figure 12.

Keyboard Shortcuts

The user interface supports the following keyboard shortcuts.

Table 3. Keyboard shortcuts

Shortcut	Action
Ctrl + Enter	Lets you switch back and forth between the Configuration Panel and the Connection Panel. If the Configuration Panel is protected with a password, you are asked for this password when you switch to the Configuration Panel.
Ctrl + D	Lets you opens the VPN Console for network debugging.
Ctrl + S	Lets you save and apply a VPN Configuration.

Connection Panel Screen

The Connection Panel screen enables you to open, close, and receive clear information about every tunnel that has been configured. If a network administrator has configured the VPN tunnels, the end user needs access to the Connection Panel screen only to open and close tunnels.

The Connection Panel screen consists of the following components:

- An animated network diagram that shows information about the current tunnel (at the top of the screen)
- A list of all configured tunnels with buttons to open and close the tunnels (below the network diagram)
- A link back to the Configuration Panel screen (at the left bottom of the screen)

You can switch back and forth between the Connection Panel screen and the Configuration Panel screen by using the **Ctrl** + **Enter** shortcut.

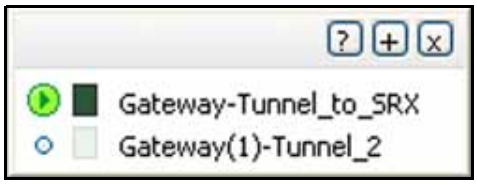


Figure 13.

Configuration Panel Screen

The Configuration Panel screen enables you to configure VPN tunnels, and consists of the following components:

- Main menu (at the top of the screen)
- The Save and Apply buttons in the left column of the screen
- A tree list pane (in the left column of the screen) that contains the Global Parameters button and all authentication phase names (that is, phase 1 names) with their associated IPSec configuration names (that is, phase 2 names)
- A configuration pane (in the right column of the screen) that shows the associated settings for each tree level
- Status bar (at the bottom of the screen)

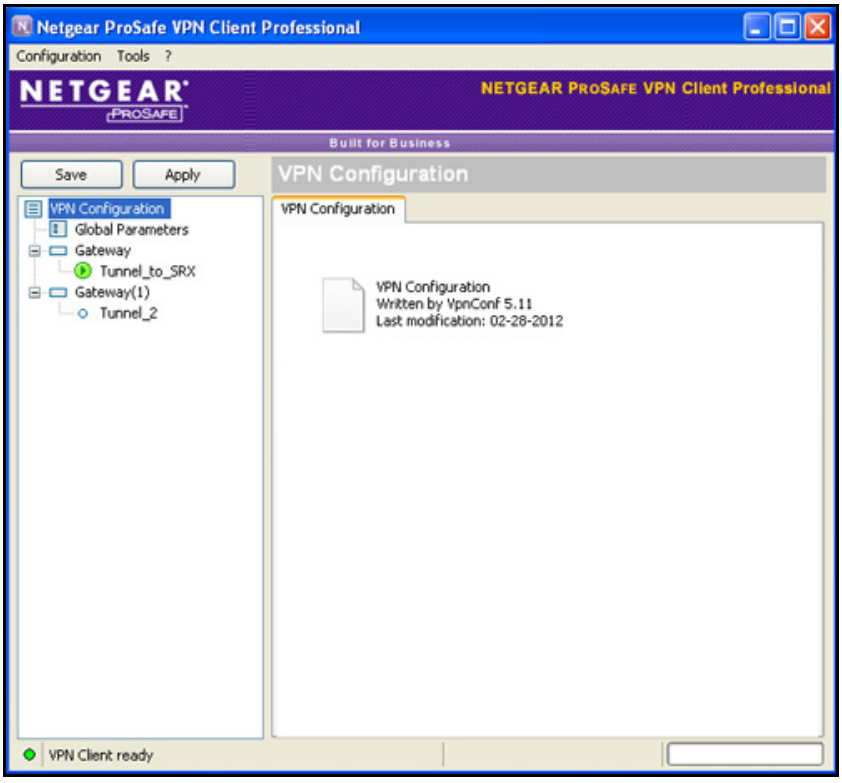


Figure 14.

You can drag and drop a VPN configuration file (that is, a file with a .tgb extension) onto the Configuration Panel screen to easily apply a new VPN configuration. If a tunnel is configured to be opened when the VPN Client starts (see *Advanced IPSec Configuration* on page 55), the tunnel is immediately opened when you click **Save** or **Apply** to apply the new VPN configuration.

Main Menu

The main menu lets you make the following selections:

- **Configuration**. Lets you import and export a VPN configuration, select the location of the VPN configuration (locally stored on the computer or on a USB drive), access the configuration wizard, and quite the VPN Client.
- **Tools**. Lets you access the Connection Panel, access the Console screen, reset the IKE settings, and configure miscellaneous preferences such as the way the VPN Client starts and the language of the VPN Client.
- **?**. Lets you access online help, check for software updates, connect to the NETGEAR website to purchase a license online, access the Activation Wizard, and access the About screen.

> ***Note:*** Some selections that are available from the Configuration menu are also available by right-clicking a component of the tree list pane in the Configuration Panel screen.

Status Bar

The status bar at the bottom displays the following information:

- The radio button indicates whether or not the VPN Client is ready for use. (Green indicates ready; gray indicates not ready.)
- The text to the right of the radio button provides the status of the VPN Client (for example, VPN Client Ready, or Apply VPN configuration).
- The progress bar at the very right displays the progress when you apply or save the configuration.

About Screen

The About screen that you can access by clicking **?** on the main menu provides the VPN Client software release number and software activation information. There is also a URL to the NETGEAR website.

Figure 15.

Options Screen

> ***Note:*** This screen is not available in the VPN Client Lite.

The Options screen, which you access by selecting **Tools > Options** from the main menu, has three tabs that provide access to the View pane, General pane, and Language pane.

View Pane: Access Control and Hidden Interface

Access control is a feature that is intended for use by a network administrator. It allows you to restrict access to the Connection Panel screen and the system tray menu with a password and to lock access to the Configuration Panel screen to prevent users from modifying the VPN configuration. Only the Configuration Panel screen can be password protected; the Connection Panel screen cannot.

When access control is enabled, you are asked for the password under the following circumstances:

- When you click (or double-click) the VPN Client icon in the system tray.
- When you switch from the Connection Panel screen to the Configuration Panel screen.
- When you start a software upgrade.

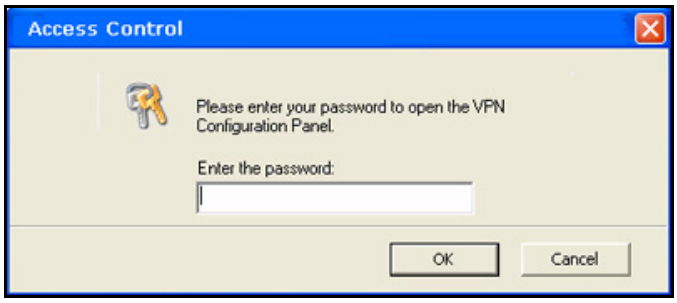


Figure 16.

You can also configure this password as an option of the software setup (see *VPN Client Software Setup Commands* on page 82).

The View pane also lets you configure the system tray menu items such as the Console, Connection Panel, and Configuration Panel, and the pop-up screens in the system tray (which are referred to as the systray sliding popup). In this way a network administrator can restrict the software access from full access to a completely hidden interface.

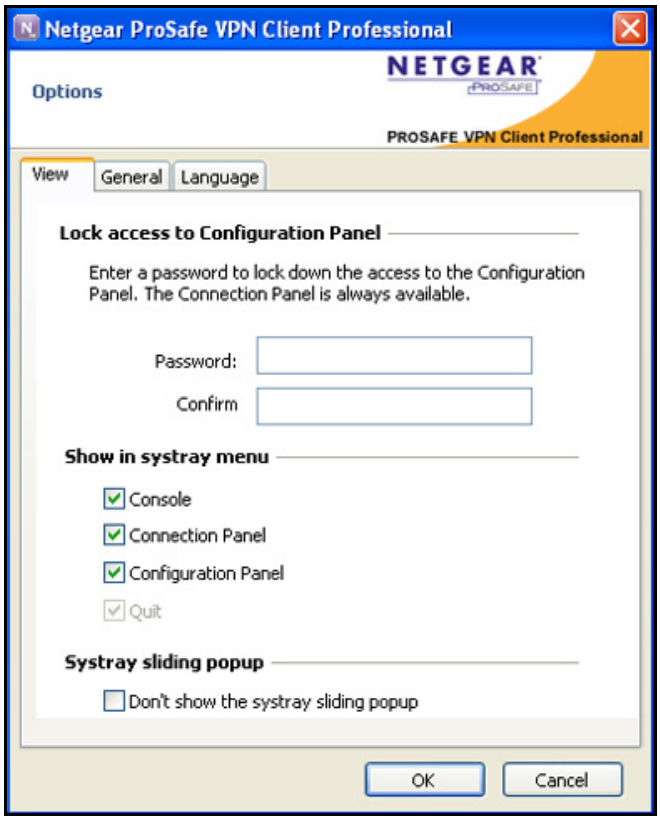


Figure 17.

➢ **To remove access control:**

1. Clear the Password and Confirm fields
2. Click **OK**.

Note: The Quit check box for the system tray menu is disabled in the standard version of the software. You can remove this check box during the software setup through the **menuitem** software setup command (see *Software Setup for System Tray Menu Items* on page 84).

When access control is enabled, you cannot open the Configuration Panel screen by double-clicking the desktop icon or by using the Start menu; when you right-click the system tray icon, the options are limited to accessing the VPN Console, opening and closing the configured tunnels, and closing the VPN Client.

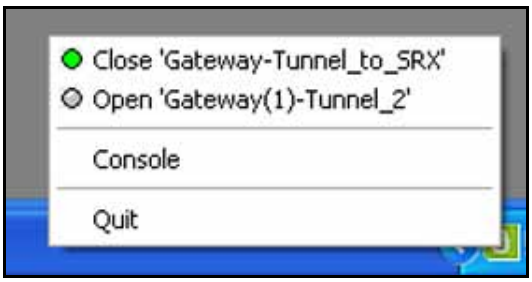


Figure 18.

General Pane

The General Pane lets you specify the following:

- VPN Client startup modes:
  - Start the VPN Client after you have logged in to Windows.
  - Do not start the VPN Client after you have logged in to Windows. In this case, you need to manually start the VPN Client or use a script to start it.

Note: You can also configure these modes in the software setup (see *VPN Client Software Setup Commands* on page 82).

- Enable or disable the detection of the interface disconnection feature. When you disable the detection of interface disconnection, the VPN Client keeps tunnels open when the network interface disconnects momentarily. This type of behavior occurs when the interface that is used to open tunnels is unstable, such as Wi-Fi, GPRS, and 3G interfaces.

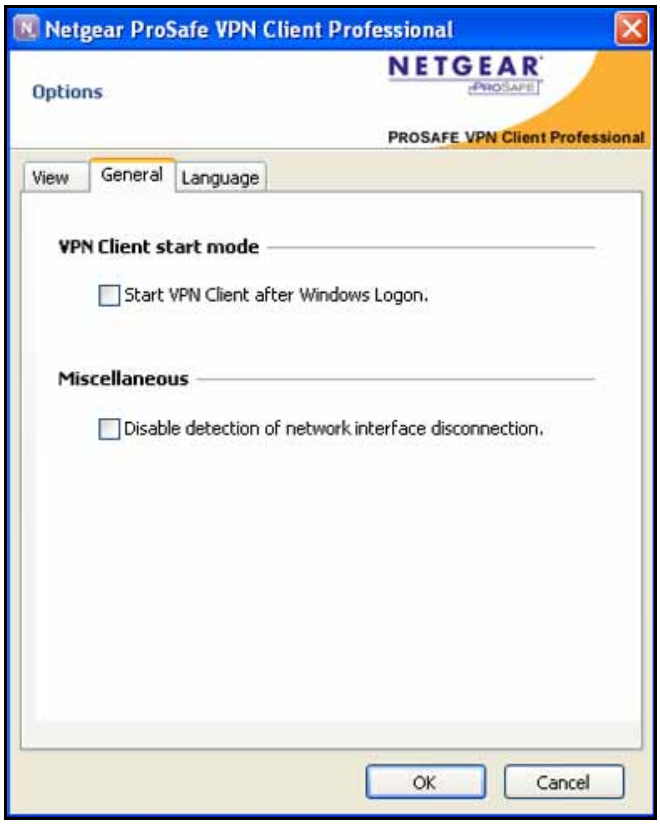


Figure 19.

Language Pane

The Language pane lets you change the VPN Client language without having to restart the VPN Client. You can also manually edit the translation in a very easy way, or even translate an existing language into another language that is not yet supported on the VPN Client to create a new localization.

For a list of the supported languages, see *Table 1* on page 8.

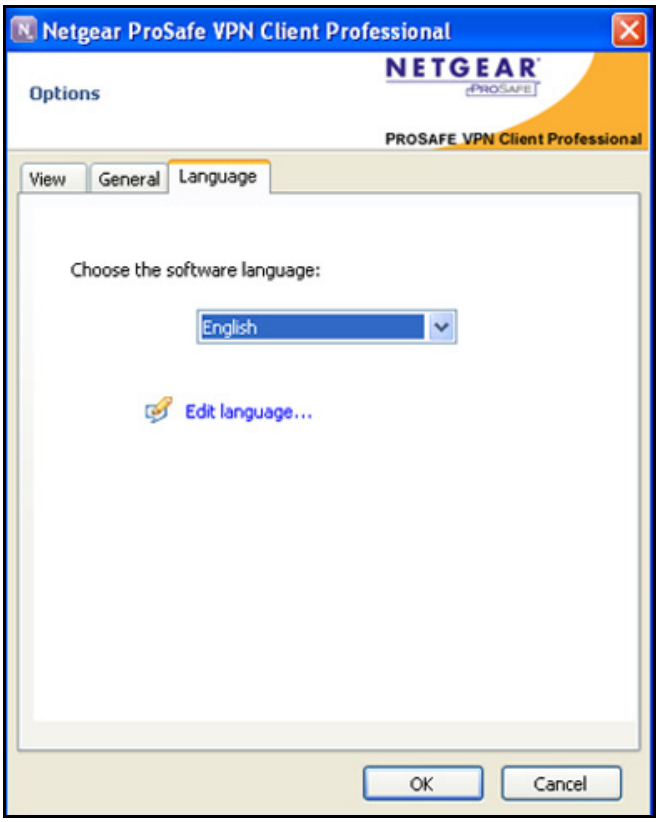


Figure 20.

➢ **To edit the translation:**

1. Click **Edit language**. The Edit language screen displays (see the next figure).
2. Select a row. A popup screen displays and shows the following four columns:
   - line number
   - **ID**. The name of the string.
   - **Original**. The string in English.
   - **Translation**. The translated string.
3. Enter your alternate translation in the popup screen, and click **Ok**.
4. Click **Save** to save the .lng file in the Language folder of the VPN Client software directory. Click **Apply** to immediately show the new translation in the user interface.

   Note: *The saved file is added as a new selection in the language drop-down list of the Language pane. The name of the new selection is the name of the original language followed by an exclamation mark. For example, if you make changes to the English language file, the new language option that is shown in the drop-down list is English!*

5. Click **Quit** to close the Language pane.

During translation, do not change the following characters, which are generic expressions:

- “%s” is replaced by a string
- “%d” is replaced by a number
- “\n” stands for carriage return
- “&” underlines the characters that follow it

IDS_DATE_FORMAT is “%m-%d-%Y”. Modify the date only if you know the appropriate syntax. Do not translate IDS_SC_P11_3.

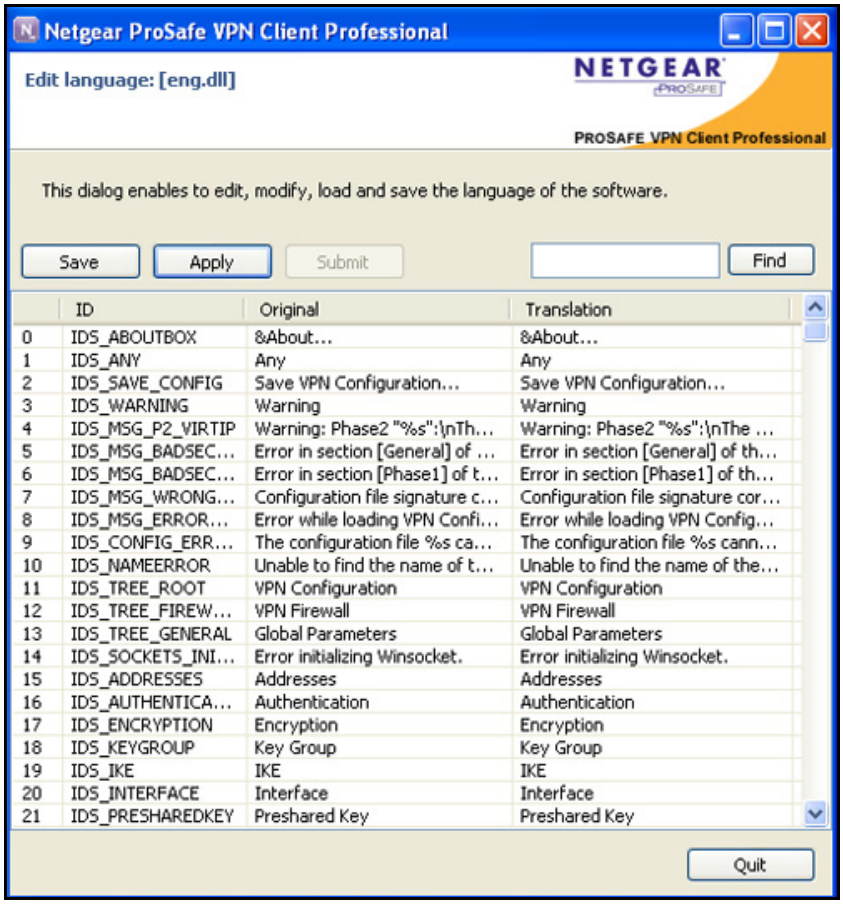


Figure 21.

Wizards

There are several wizards available:

- **VPN Configuration Wizard**. Access this wizard by selecting **Configuration > Wizard** from the main menu (for more information, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 41).
- **Software Activation Wizard**. Access this wizard by selecting **? > Activation Wizard** from the main menu (for more information, see *Software Activation Wizard* on page 15).

- **USB Mode Wizard**. Access this wizard by selecting **File > Move to USB Drive** from the main menu (for more information, see *USB Mode* on page 62).
- **Certificate Export Wizard**. Access this wizard by selecting **View Certificate** on the Certificate pane, selecting the **Details** tab on the View Certificate screen, and then selecting **Copy to File** (for more information, see *View Certificate Details* on page 68).

VPN Console Active Screen

You can access the VPN Console Active screen from the system tray menu, from the Console button on the Configuration Panel screen, or by selecting **Tools > Console** from the main menu of the Console Panel screen. Use the VPN Console Active screen to analyze VPN tunnels, which can be useful if you are a network administrator and have to set up a network.

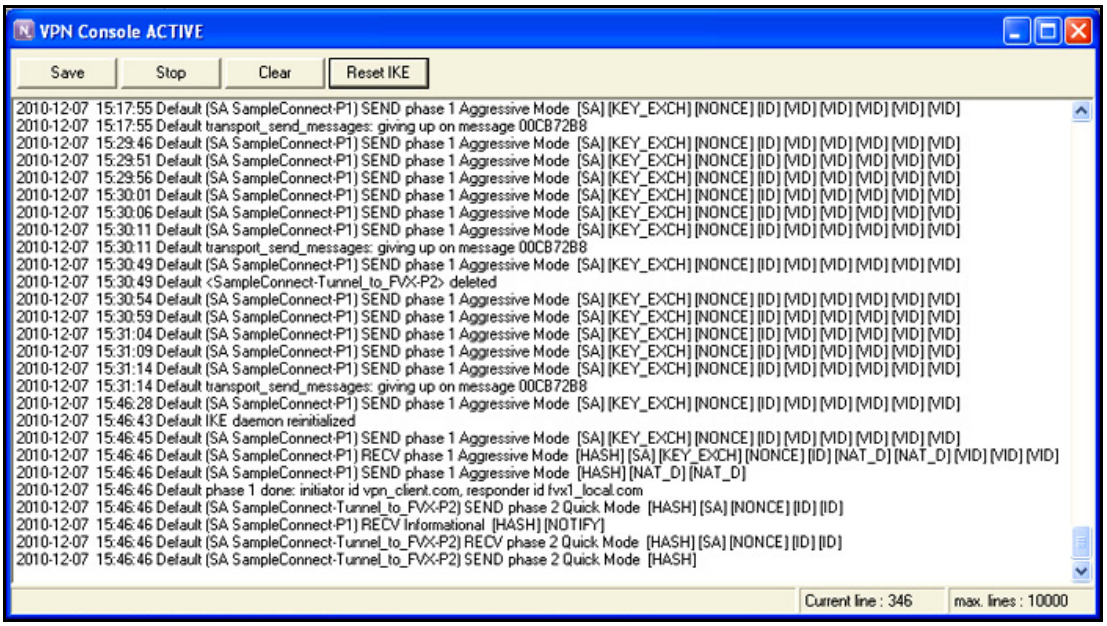


Figure 22.

The buttons on the VPN Console Active screen have the following functions:

- **Save**. Saves the current logs in a file without overwriting previous logs.
- **Start** or **Stop**. Starts or stops the collection of logs. Only one of these buttons is displayed onscreen at a time.
- **Clear**. Removes the content from the screen.
- **Reset IKE**. Restarts the IKE process.

Note: To enable debug mode, which is also referred to as trace mode, press **Ctrl+Alt+D**. Note that the trace logs become large rather quickly.

Basic Tasks

4

This chapter describes some basic tasks of the VPN Client. These tasks are described in more detail in other chapters. This chapter includes the following sections:

- *Open a VPN Tunnel*
- *Easily Import a VPN Configuration*
- *Specify a Certificate for User Authentication*
- *Open a VPN Tunnel before Windows Logon*

Open a VPN Tunnel

You can open a tunnel only after the VPN configuration has been specified.

➢ **To open a tunnel, use one of the following five methods:**

- **Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:
  - Click the IPSec configuration name (by default, Tunnel) and press **Ctrl + O.**
  - Right-click the IPSec configuration name (by default, Tunnel) and select **Open tunnel**.

  For more information, see *Chapter 6, Configuration Panel Screen Tasks*.
- **Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen. Perform *one* of the following tasks:
  - Double-click the connection name (by default, Gateway-Tunnel).
  - Right-click the connection name (by default, Gateway-Tunnel) and click **Open tunnel**.
  - Click the connection name (by default, Gateway-Tunnel) and press **Ctrl + O**.

  For more information, see *Chapter 5, Connection Panel Screen Tasks*.
- **System-tray icon**. Right-click the system tray icon and click the IPSec configuration name (by default, Tunnel). For more information, see *User Interface Elements* on page 21.

- **VPN configuration icon**. Double-click on a VPN configuration icon on your desktop or in an email attachment. For information about how to create a VPN configuration icon, see *VPN Configuration Management* on page 76.
- **CLI**. Use the command-line interface (CLI). For more information, see *Open or Close VPN Tunnels* on page 87.

➢ **To enable a tunnel to be opened automatically, select one or more of the following check boxes on the Advanced IPSec pane of the Configuration Panel screen:**

- Automatically open this tunnel when the VPN Client starts after login
- Automatically open this tunnel when USB stick is inserted
- Automatically open this tunnel on traffic detection

For more information, see *Advanced IPSec Configuration* on page 55.

Easily Import a VPN Configuration

You can create various VPN configurations on the Windows desktop and open a tunnel by double-clicking a VPN configuration icon (that is, a file with a .tgb extension).

➢ **To create a VPN configuration shortcut icon on the desktop:**

1. Configure a tunnel on the Configuration Panel screen (see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 41 or *Manually Create a VPN Tunnel Connection* on page 44).
2. Configure the tunnel to automatically open when the VPN Client starts after login (see *Advanced IPSec Configuration* on page 55).
3. Export the VPN configuration onto your computer desktop (see *Import or Export a VPN Configuration* on page 76).

Specify a Certificate for User Authentication

➢ **To configure new authentication settings (phase 1 settings) and an associated IPSec configuration (phase 2 settings), and then specify a certificate for the tunnel:**

1. Create new authentication settings (phase 1 settings, see *Configure Authentication* on page 45) and configure the advanced settings (see *Configure Advanced Authentication* on page 47).

Figure 23.

2. Add a new IPSec configuration (phase 2 settings, see *Configure IPSec* on page 52) and configure the advanced settings (see *Advanced IPSec Configuration* on page 55).

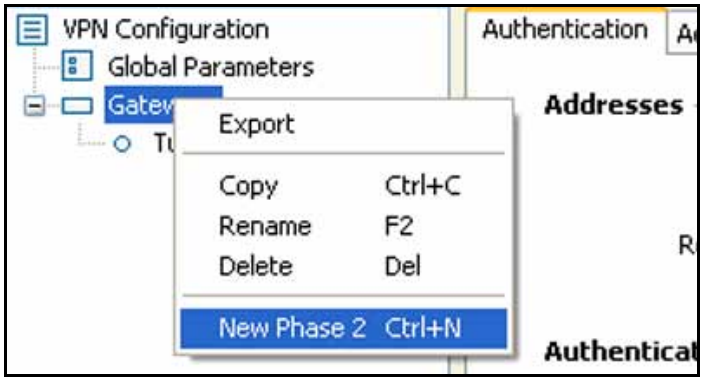


Figure 24.

3. Go back to the Authentication pane, and select the **Advanced** tab. The Advanced authentication pane displays.
4. Select the **Certificate** radio button.

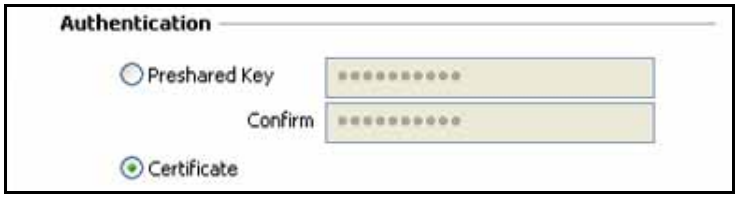


Figure 25.

The Certificate pane displays automatically (see the following figure).

5. From the list of certificates, specify a certificate by selecting its radio button (see *Assign Certificates* on page 67). You can also click **Import Certificate** to import a new certificate (see *Import Certificates* on page 69), and then click **OK**.
6. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

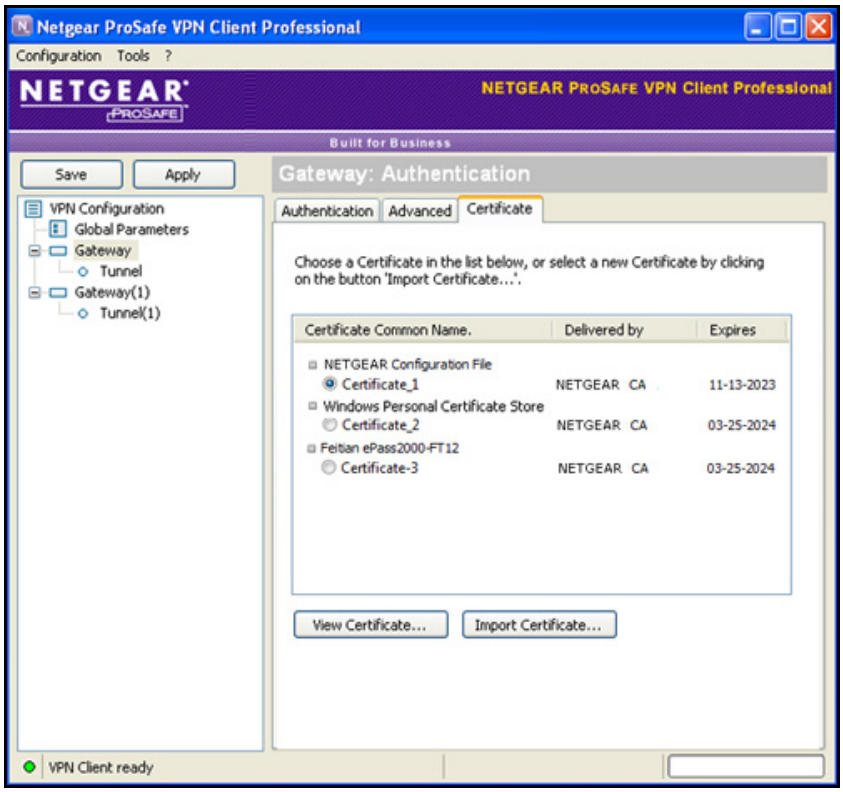
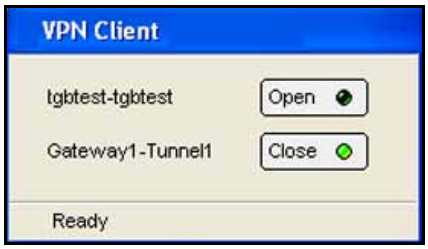


Figure 26.

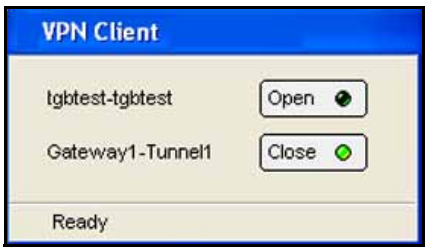
Open a VPN Tunnel before Windows Logon

You can manually or automatically open one or more VPN tunnels before Windows login by using a Windows logon technology that is referred to as Credential Providers in Vista and later releases and as Gina mode in Windows 2000 and Windows XP.

➢ **To manually open a VPN tunnel before Windows logon:**

Settings	VPN Client Behavior
1. Open the Advanced IPSec pane. 2. Select the **Enable before Windows logon** check box. 3. Ensure that the **Automatically open this tunnel on traffic detection** check box is cleared. For more information, see *Advanced IPSec Configuration* on page 55.	Before Windows logon, the following popup screen displays to allow you to open the required VPN tunnel.  The popup screen lists all VPN tunnels for which you have selected the Enable before Windows logon check box on the Advanced IPSec pane.

➢ To automatically open a VPN tunnel before Windows logon:

Settings	VPN Client Behavior
1. Open the Advanced IPSec pane. 2. Select the **Enable before Windows logon** check box. 3. Select the **Automatically open this tunnel on traffic detection** check box. For more information, see *Advanced IPSec Configuration* on page 55.	Before Windows logon, the following popup screen displays to show the VPN tunnels that are opened automatically.  The popup screen lists all VPN tunnels for which you have selected the Enable before Windows logon check box on the Advanced IPSec pane.

> ***Note:*** To enable a VPN tunnel to automatically open on traffic detection *after* Windows logon, select the **Automatically open this tunnel on traffic detection** check box and ensure that the **Enable before Windows logon** check box is cleared.

The following information applies to tunnels for which you have selected the Enable before Windows logon check box on the Advanced IPSec pane:

- You cannot hide the popup screen that appears before Windows logon.
- If two tunnels have been configured to automatically open on traffic detection but only one tunnel is configured to be enabled before Windows logon, both tunnels might open automatically before Windows logon when the IKE services are running.
- Scripts that you might have configured are disabled.
- The VPN Client cannot function in USB mode (see *USB Mode* on page 62).
- The Mode Config feature is disabled, so you might have to specify DNS or WINS server addresses (see *Advanced IPSec Configuration* on page 55).
- When extended authentication (XAUTH) is enabled (see *Extended Authentication* on page 51), a popup screen displays when tunnels open to enable you to enter the login name and password.
- When you use a USB token or smart card, a popup screen displays when tunnels open to enable you to enter the PIN code.

Connection Panel Screen Tasks

5

This chapter describes the Connection Panel screen basics.

The Connection Panel screen enables you to open and close each tunnel that has been configured. If a network administrator has configured the VPN tunnels, the end user needs access only to the Connection Panel to open and close tunnels.

➢ **To open the Connection Panel screen, use one of the following two methods:**

- Select **Tools > Connection Panel** from the main menu on the Configuration Panel screen.
- Right-click the system tray icon and select **Connection Panel**.

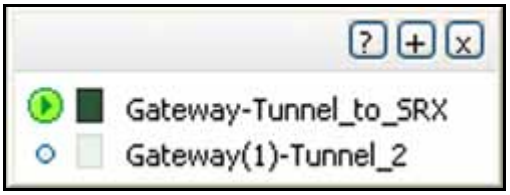


Figure 27.

The Connection Panel screen consists of the following components:

- For each tunnel, the following components:
  - An icon that shows whether or not the tunnel is open: a small circular gray icon indicates that the tunnel is closed; a large circular green icon with an arrow in the middle indicates that the tunnel is open.
  - A rectangular traffic gauge that shows the traffic volume passing through the tunnel.
  - The connection name (tunnel name) in the format authentication phase name–IPSec configuration name.
- Three icons in the upper right corner:
  - **?**. Opens the About screen.
  - **+**. Opens the Configuration Panel screen.
  - **x**. Closes the Connection Panel screen.

You can switch back and forth between the Connection Panel screen and the Configuration Panel screen by using the **Ctrl + Enter** shortcut.

- **To open a selected connection (tunnel), use one of the following three methods:**
  - Double-click the tunnel (anywhere, the icon, gauge, or name).
  - Right-click the tunnel and then click **Open tunnel**.
  - Click on the tunnel and press **Ctrl + O**.
- **To close a selected connection (tunnel), use one of the following three methods:**
  - Double-click the tunnel (anywhere, the icon, gauge, or name).
  - Right-click the tunnel and then click **Close tunnel**.
  - Click on the tunnel and press **Ctrl + C**.

Configuration Panel Screen Tasks

6

This chapter describes the Configuration Panel screen. This chapter includes the following sections:

- *Use the Configuration Wizard to Create a VPN Tunnel Connection*
- *Manually Create a VPN Tunnel Connection*
- *Authentication or Phase 1*
- *IPSec or Phase 2*
- *Global Parameters*
- *USB Mode*
- *Certificate Management*
- *VPN Configuration Management*

Use the Configuration Wizard to Create a VPN Tunnel Connection

The VPN Client provides a Configuration Wizard that lets you create a VPN configuration in three easy steps. This Configuration Wizard is designed for remote computers that need to be connected to a corporate LAN through a VPN gateway and for peer-to-peer connections.

The configuration in the following figure has the following characteristics:

- The remote computer has a dynamically provided public IP address.
- The remote computer connects to the corporate LAN behind a VPN gateway that has a DNS address with the name gateway.mydomain.com.
- The corporate LAN address is 192.168.1.xxx, that is, the remote computer must reach a server with the IP address 192.168.1.100.

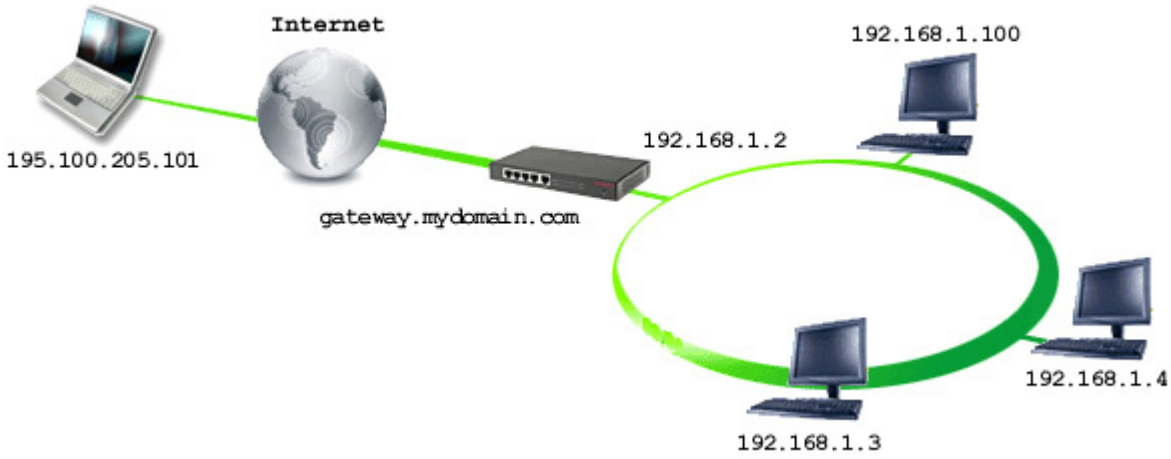


Figure 28.

➢ **To create a VPN tunnel connection between the remote computer and the corporate LAN:**

1. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The VPN Client Configuration Wizard Step 1 of 3 screen displays:

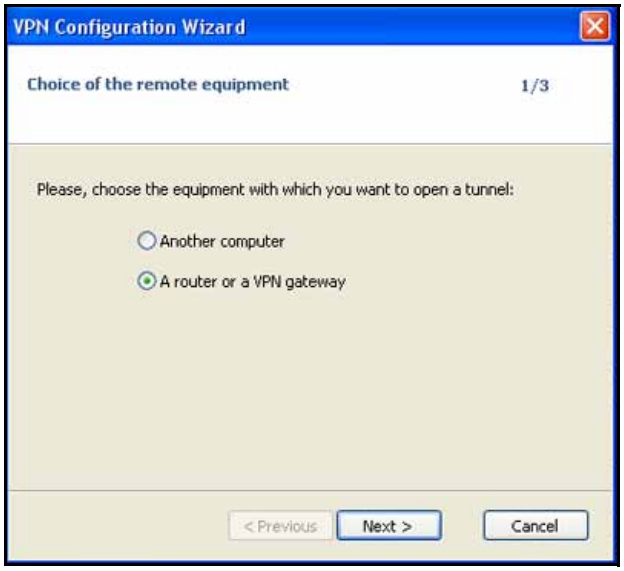


Figure 29.

2. Select the equipment to connect to. The options are **Another computer** and **A router or a VPN gateway**. In this configuration, select the **A router or a VPN gateway** radio button.
3. Click **Next**. The VPN Client Configuration Wizard Step 2 of 3 screen displays:

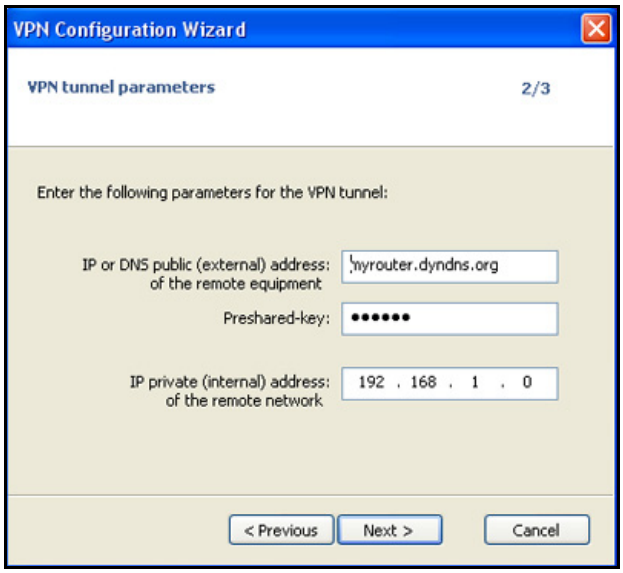


Figure 30.

4. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. The public (WAN) IP address of the remote gateway. In this example, enter **gateway.mydomain.com**.
   - **Preshared key**. The preshared key that must also be defined on the remote gateway.
   - **IP private (internal) address of the remote network**. The IP address of the remote network. In this example, enter **192.168.1.0**.
5. Click **Next**. The VPN Client Configuration Wizard Step 3 of 3 screen displays:

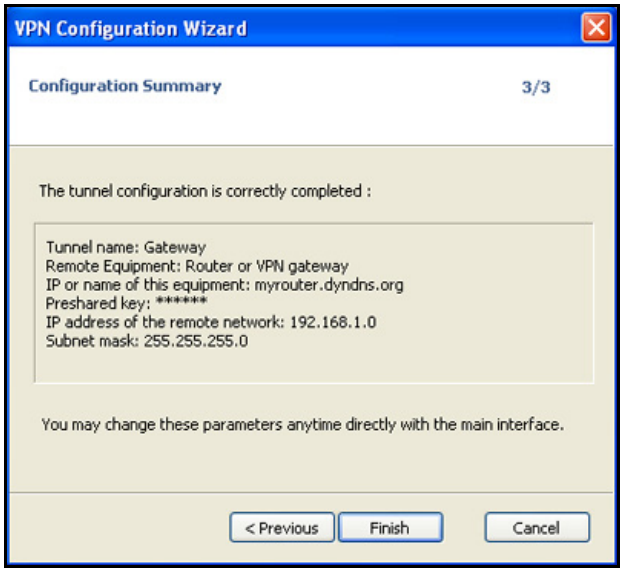


Figure 31.

This screen is a summary screen of the new VPN configuration. If required, you can specify other settings such as certificates and virtual IP addresses on the Configuration Panel screen.

6. Click **Finish**.

➢ **To open the newly created tunnel:**

1. From the main menu on the Configuration Panel screen, select **Tools > Connection Panel**.
2. Double-click the newly created tunnel (Gateway-Tunnel), or right-click the newly created tunnel, and then click **Open Tunnel**.

Manually Create a VPN Tunnel Connection

➢ **To manually create a VPN tunnel from the Configuration Panel screen:**

1. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration** and select **Reset**.

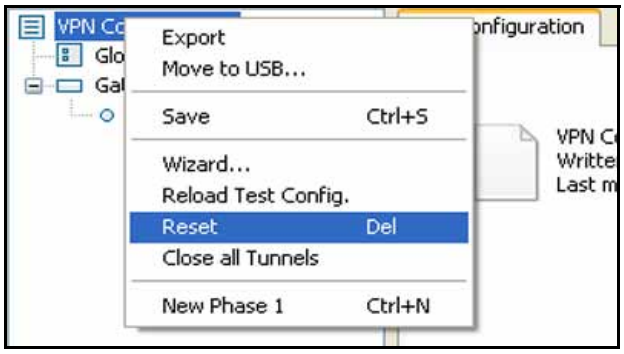


Figure 32.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration** and select **New Phase 1**.

Figure 33.

3. The Authentication pane displays in the right column of the Configuration Panel screen. Configure the authentication that enables you to connect to the remote gateway or computer as explained in *Authentication or Phase 1* on page 45.

4. In the tree list pane of the Configuration Panel screen, right-click **Gateway** (which is the default name of the new phase 1 configuration) and select **New Phase 2**.

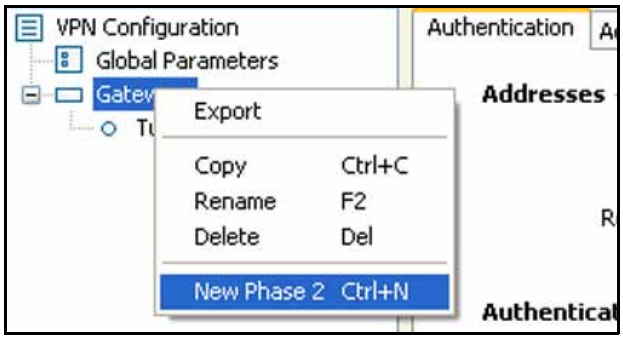


Figure 34.

5. The IPSec pane displays in the right column of the Configuration Panel screen. Specify the IPSec configuration that enables the VPN Client to communicate securely with the remote gateway or computer as explained in *IPSec or Phase 2* on page 52.
6. Click **Apply** for immediate use.
7. Click **Save** for future use.
8. Right-click the tunnel that you just configured, and click **Open Tunnel** to open the new VPN tunnel.

Authentication or Phase 1

The Authentication pane that opens in the Configuration Panel screen lets you specify the settings for the authentication phase, which is also referred to as phase 1 or as the Internet Key Exchange (IKE) negotiation phase. The purpose of phase 1 is to negotiate IKE policy sets, authenticate the peers, and set up a secure channel between the peers. As part of phase 1, each end system must identify and authenticate itself to the other.

You can specify settings for several authentication phases, enabling one computer to establish IPSec VPN connections with several gateways or other computers (peer-to-peer connections).

Configure Authentication

➢ **To create new authentication settings or edit existing authentication settings:**

1. Take one of the following actions:
   - Create new authentication settings: In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, select **New Phase 1**, and then click on the new authentication phase name.
   - Edit existing authentication settings: In the tree list pane of the Configuration Panel screen, select an existing authentication phase name (for example, Gateway in the following figure).

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

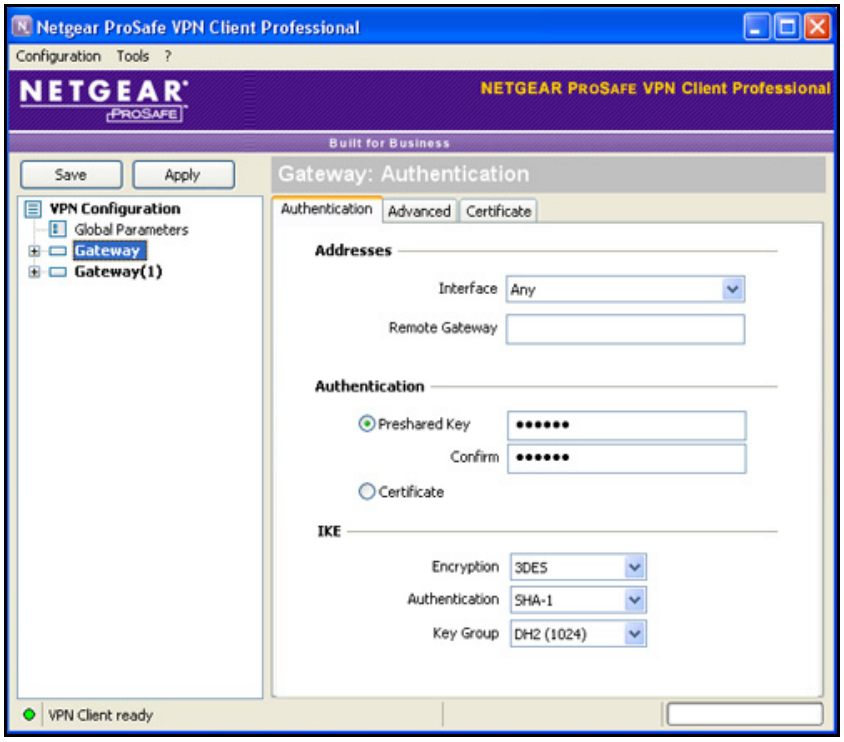


Figure 35.

2. To change the name of the authentication settings (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Enter a new name.
   d. Click anywhere in the tree list pane.
3. Configure the settings as explained in the following table.

Table 4. Authentication settings (phase 1 settings)

Setting	Description
Interface	From the Interface drop-down list, select the IP address of the network interface of the computer through which the VPN connection is established. If the IP address changes (when it is received dynamically from an ISP or router), select **Any**. **Note:** If your selection of the Interface drop-down list refers to an IP address that does not exist on the computer, Any is used automatically.
Remote Gateway	Enter the IP address or DNS address of the remote gateway (in the example onscreen, myrouter.dyndns.org). This field is mandatory.
Preshared Key	Enter the password or key that is shared with the remote gateway. You need to enter the same password or key in the Confirm field.

Table 4. Authentication settings (phase 1 settings) (continued)

Setting	Description	
Certificate	This selection is optional. The X509 certificate that is used by the VPN Client. On the IPSec pane, click the **Certificate** tab to open the Certificate pane that lets you select the certificate source. You can use a PEM file, PKCS#21 file, smart card, or token, or a certificate from the Personal Certificate Store. Specify only one certificate per tunnel. For information about certificates, see *Certificate Management* on page 66.	
IKE	Encryption	The encryption algorithm that is used during the authentication phase. Select one of the following from the drop-down list: • **DES**. • **3DES**. This is the default setting. • **AES128**. • **AES192**. • **AES256**.
	Authentication	The authentication algorithm that is used during the authentication phase. Select one of the following from the drop-down list: • **MD5**. • **SHA-1**. This is the default setting. • **SHA-256**.
	Key Group	The Diffie-Hellman key length that is used during the authentication phase. Select one of the following from the drop-down list: • **DH1 (768)**. • **DH2 (1024)**. This is the default setting. • **DH5 (1536)**. • **DH14 (2048)**.

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure Advanced Authentication

Note: For authentication settings (phase 1 settings), the advanced configuration settings apply to all its associated IPSec configurations (phase 2 settings).

➢ **To configure advanced authentication settings:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to configure the advanced settings (for example, Gateway in the following figure). The Authentication pane displays.
2. In the Authentication pane, click the **Advanced** tab. The Advanced authentication pane displays:

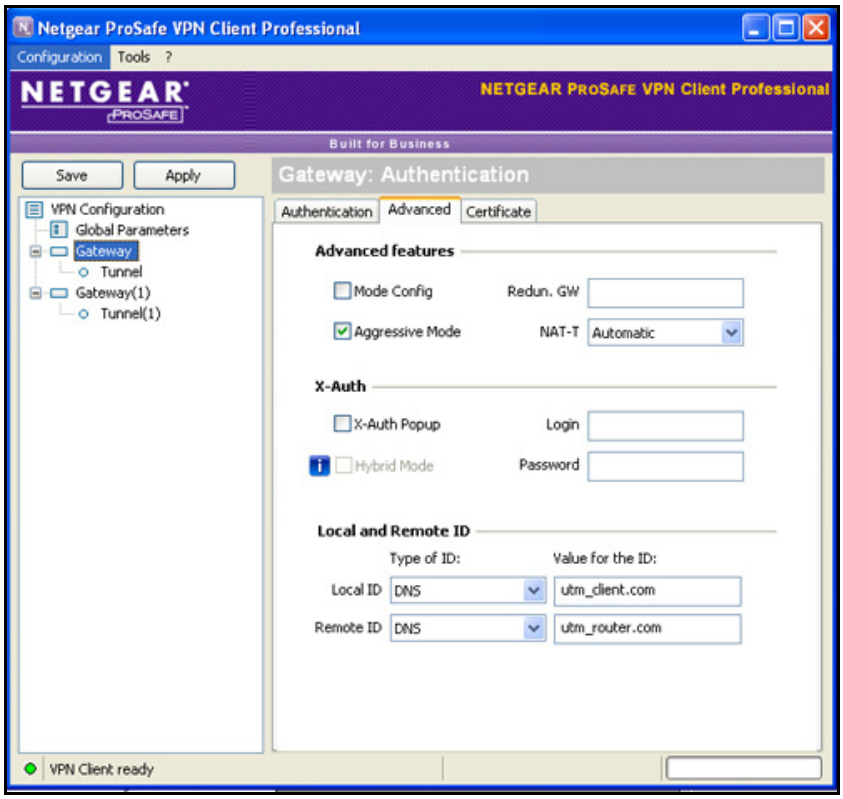


Figure 36.

3. Configure the settings as explained in the following table.

Table 5. Advanced authentication settings

Setting	Description
Advanced features	
Mode Config	Select the **Mode Config** check box to enable the Mode Config feature that allows the VPN Client to receive VPN configuration information from the remote VPN gateway. (The remote VPN gateway must support the Mode Config feature.) When the Mode Config feature is enabled, the following information is negotiated between the VPN Client and the remote VPN gateway during the authentication phase: • Virtual IP address of the VPN Client • DNS server address (optional) • WINS server address (optional) **Note:** The virtual IP address that is issued by the remote VPN gateway is displayed in the VPN Client Address field on the IPSec pane with the IPSec tab selected. **Note:** If the Mode Config feature is not available or not supported on the remote VPN gateway, see the information in *Advanced IPSec Configuration* on page 55 to manually specify the DNS and WINS server addresses on the VPN Client.

Table 5. Advanced authentication settings (continued)

Setting	Description
Aggressive Mode	The Aggressive Mode check box is selected by default to enable the VPN Client to use aggressive mode as the negotiation mode with the remote VPN gateway. Clear the check box to disable aggressive mode.
Redund.GW	Enter the IP address or URL of an alternate VPN gateway in the Redund.GW field to enable the VPN Client to open an IPSec tunnel with an alternate gateway when the primary VPN gateway is down, goes down, or stops responding. An alternate gateway is used under the following circumstances: • If the VPN Client cannot contact the primary gateway to establish a tunnel. After several attempts (determined by the value in the Retransmission field—the default is 5 attempts—in the Parameters pane of the Configuration Panel screen (see *Global Parameters* on page 60), the VPN Client uses the alternate gateway as the new tunnel endpoint. The interval between two attempts is about 10 seconds. • If a tunnel is successfully established with the primary gateway with the Dead Pear Detection (DPD) feature (see *Global Parameters* on page 60) but the primary gateway stops responding to DPD messages. **Note:** The same connection rules apply if the alternate gateway goes down or stops responding. This means that the VPN Client could switch between the primary and alternate gateways until you click **Save** or **Apply** or close and exit the VPN Client. **Note:** If the primary gateway can be reached but tunnel establishment fails (that is, there are VPN configuration errors), the VPN Client does not attempt to establish a tunnel with the alternate gateway. In this case you must first resolve the configuration errors.
NAT-T	From the NAT-T drop-down list, select one of the following NAT Traversal (NAT-T) modes: • **Automatic**. Enables the VPN Client and VPN gateway to negotiate NAT-T. This is the default setting. • **Forced**. Enables the VPN Client to force NAT-T by encapsulating IPSec packets into UDP frames, thereby allowing packet traversal through intermediate NAT routers. • **Disabled**. Prevents the VPN Client and VPN gateway from negotiating NAT-T.
X-Auth	
X-Auth Popup	Extended authentication (XAUTH) is an extension to the IKE protocol. If extended authentication is configured on the gateway, select the **X-Auth Popup** check box to enable a popup screen in which the login name and password can be entered during the authentication phase. This popup screen displays each time when authentication is required to open a tunnel with a remote VPN gateway. If XAUTH authentication fails, the tunnel establishment fails too. **Note:** If you enter a name in the Login field and a password in the Password field, the popup screen does not display, and the tunnel is establishes if the credentials match those on the gateway. However, this defeats the purpose of extended authentication. NETGEAR recommends that you do not enter a name and password on the Advanced authentication pane but let the user enter these credentials. For more information, see *Extended Authentication* on page 51.

Table 5. Advanced authentication settings (continued)

Setting	Description
Hybrid Mode	Select the **Hybrid Mode** check box to enable this mode, and enter a name in the Login field and a password in the Password field. **Note:** Hybrid Mode requires you to configure a certificate for the authentication phase (see *Configure Authentication* on page 45) and to select Extended authentication (XAUTH), that is, the X-Auth Popup check box. Hybrid mode is an authentication method that is used within the authentication phase. Hybrid mode assumes an asymmetry between the authenticating entities. One entity, typically an edge device (for example, a firewall), authenticates using standard public key techniques (in signature mode), while the other entity, typically a remote user, authenticates using challenge response techniques. At the end of the authentication phase, these authentication methods are used to establish an IKE SA that is unidirectionally authenticated. To ensure that the IKE is bidirectionally authenticated, the authentication phase is immediately followed by an extended authentication (XAUTH) to authenticate the remote user. The use of these authentication methods is referred to as hybrid authentication mode. **Note:** The VPN Client implements the RFC draft-ietf-ipsec-isakmp-hybrid-auth-05.txt.
Local and Remote ID	
Local ID	The local ID is the identity that the VPN Client transmits to the VPN gateway during the authentication phase. From the Local ID drop-down list, select one of the following types of IDs, and enter the associated value for the ID in the field to the right: • **IP Address**. Enter a standard IP address (for example, 195.100.205.101). • **DNS**. Enter a fully qualified domain name (FQDN) (for example, mydomain.com). • **DER ASN1 DN**. Enter a certificate issuer (for more information, see *Certificate Management* on page 66). If you do not enter a certificate, the IP address of the VPN Client is used. • **Subject from X509**. These fields are automatically set when you import a certificate (see *Import Certificates* on page 69). **Note:** If a VPN tunnel closes because the computer has changed its IP address, the VPN tunnel does not reopen automatically when the network becomes available again.
Remote ID	The remote ID is the identity that the VPN Client receives from the VPN gateway during the authentication phase. From the Remote ID drop-down list, select one of the following types of IDs, and enter the associated value for the ID in the field to the right: • **IP Address**. Enter a standard IP address (for example, 203.0.113.4). • **DNS**. Enter a fully qualified domain name (FQDN) (for example, gateway.mydomain.com). • **DER ASN1 DN**. Enter a certificate issuer (for more information, see *Certificate Management* on page 66). If you do not enter a certificate, the IP address of the VPN gateway is used.

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Extended Authentication

IKE is an important element of the Public Key Infrastructure (PKI) that defines how security credentials are exchanged over the IPSec tunneling protocol. For extended authentication (XAUTH), IPSec negotiation requires the definition of a login name and password on the remote VPN gateway. The VPN Client supports several authentication protocols, including CHAP and one-time password (OTP).

➢ **To configure XAUTH and enable a user enter credentials:**

1. Configure extended authentication on the remote VPN gateway.
2. Select the **X-Auth Popup** check box on the Advanced authentication pane of the VPN Client.
3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
4. The user opens a tunnel.
5. The user enters credentials on the XAUTH popup screen (see the following figure). The credentials need to match those on the remote VPN gateway.

Note: The XAUTH popup screen displays each time when authentication is required to open a tunnel with a remote VPN gateway. If XAUTH authentication fails, the tunnel establishment fails too.

Note: In a multiple VPN tunnel configuration, the name of the VPN tunnel displays in the popup screen.

Figure 37.

The user has some time to enter the credentials. If the time allowed to enter XAUTH credentials expires, a warning screen displays and the user has to reopen the VPN tunnel. The expiration time depends on the settings of the X-Auth timeout field on the Parameters pane of the Connection Panel screen (see *Global Parameters* on page 60).

Figure 38.

The way that credentials are verified depends on the VPN gateway. When a VPN gateway detects an incorrect login name or password, one of the following actions can occur:

- The XAUTH screen displays again.
- A popup warning similar to the following one alerts the user to try to open the VPN tunnel again.

Figure 39.

IPSec or Phase 2

The purpose of the IPSec configuration, which is also referred to as phase 2, is to negotiate the IP security settings that are applied to the traffic that goes through the tunnels.

> ***Note:*** You can create several IPSec configurations (phase 2 settings) for a single set of authentication settings (phase 1 settings).

Configure IPSec

➢ **To create a new IPSec configuration or edit an existing IPSec configuration:**

1. Take one of the following actions:
   - Create a new IPSec configuration: In the tree list pane of the Configuration Panel screen, right-click an existing authentication phase name (for example, Gateway in the following figure), and then select **New Phase 2**.
   - Edit an existing IPSec configuration: In the tree list pane of the Configuration Panel screen, click an existing IPSec configuration name (for example, Tunnel in the following figure).

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.

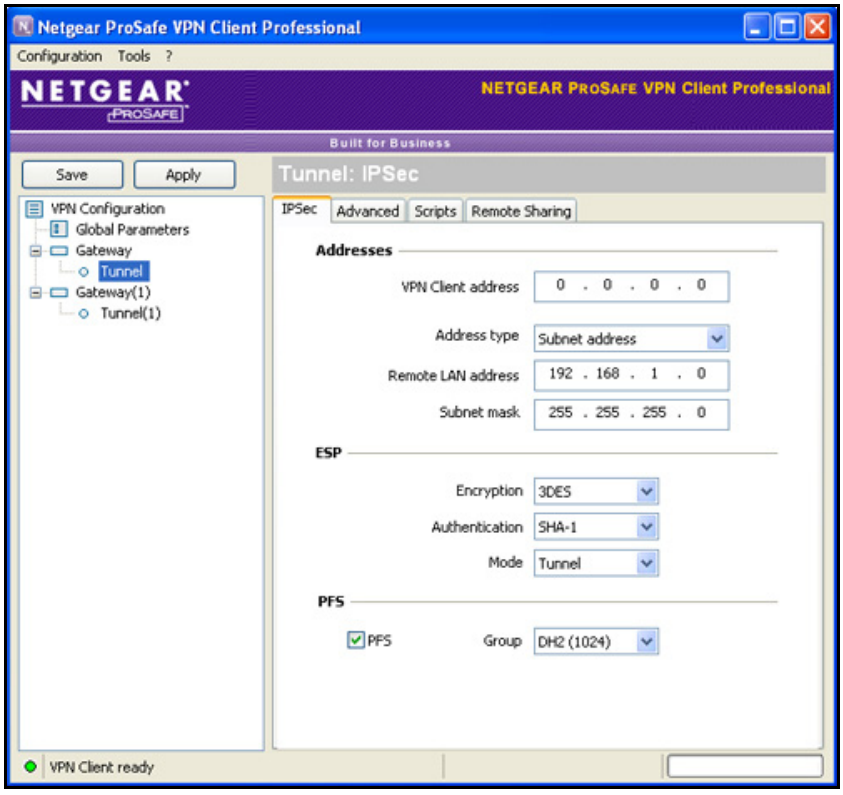


Figure 40.

2. To change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Enter a new name.
   d. Click anywhere in the tree list pane.

3. Configure the settings as explained in the following table.

Table 6. IPSec configuration settings (phase 2 settings)

Setting	Description		
VPN Client address	Enter the virtual IP address that is used by the VPN Client in the remote LAN; the computer (for which the VPN Client opened a tunnel) appears in the LAN with this IP address. This IP address can belong to the remote LAN subnet. You can also enter **0.0.0.0** as the IP address. Both the local IP address of your computer and the remote LAN address can be part of the same subnet. To enable such a configuration, select the **Automatically open this tunnel on traffic detection** check box on the Advanced IPSec pane (see *Advanced IPSec Configuration* on page 55). When the VPN tunnel is opened in this configuration, all traffic with the remote LAN is allowed but communication with the local network becomes impossible. **Note:** If Mode Config is enabled and the remote VPN gateway has issued an IP address to the VPN Client, the IP address is displayed in the VPN Client address field.		
Address type	From the Address type drop-down list, select the remote endpoint's type of address that the VPN Client can communicate with after the VPN tunnel has been established. Depending on your selection, the pane adjusts to display the associated address fields: • **Single address**. The remote endpoint is a single computer. Fill in the Remote host address and Subnet Mask fields. • **Subnet address**. The remote endpoint is a LAN. Fill in the Remote LAN address and Subnet Mask fields. • **Range address**. The remote endpoint is a LAN that consists of a range of addresses. Fill in the Start address and End address fields. **Note:** When you select **Range address** from the drop-down list and the **Automatically open this tunnel on traffic detection** check box on the Advanced IPSec pane (see *Advanced IPSec Configuration* on page 55), the tunnel automatically opens when traffic is detected for a specific range of IP addresses. However, this range of IP addresses must be specified in the configuration of VPN gateway.		
	Single address	Remote host address	Enter the addresses.
	Subnet address	Remote LAN address	
		Subnet Mask	
	Range address	Start address	
		End address	
ESP	Encryption	The encryption algorithm that is used during the IPSec configuration phase. Select one of the following from the drop-down list: • **DES**. • **3DES**. This is the default setting. • **AES128**. • **AES192**. • **AES256**.	

Table 6. IPSec configuration settings (phase 2 settings) (continued)

Setting	Description	
ESP (continued)	Authentication	The authentication algorithm that is used during the IPSec configuration phase. Select one of the following from the drop-down list: • **MD5**. • **SHA-1**. This is the default setting. • **SHA-256**.
	Mode	IPSec encapsulation mode. Select one of the following from the drop-down list: • **Tunnel**. The mode that is commonly used when either end of a security association (SA) is a security gateway or when both ends of an SA are security gateways that function as proxies for the hosts behind them. Tunnel mode encrypts both the payload and the entire header (UDP/TCP and IP). This is the default setting. • **Transport**. The mode in which traffic is destined for a security gateway that functions as a host. (For example, you could use transport mode for SNMP commands.) Transport mode encrypts only the payload, not the IP header.
PFS	Select the **PFS** check box to specify a Perfect Forward Secrecy (PFS) key length that is used during the IPSec configuration phase. Then, specify a group. By default, the PFS check box is selected.	
	Group	Select one of the following from the drop-down list: • **DH1 (768)**. • **DH2 (1024)**. This is the default setting. • **DH5 (1536)**. • **DH14 (2048)**.

4. As an optional step, click the **Advanced** tab to open the Advanced IPSec pane and configure the advanced settings (for more information, see the following section).
5. As an optional step, click the **Scripts** tab to open the IPSec Scripts pane and specify scripts. For information, see *Script Configuration* on page 57.
6. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
7. As an optional step, in the tree list pane, right-click the IPSec configuration name (for example, Tunnel), and then click **Open Tunnel** to open the newly configured tunnel. (When the tunnel is opened, this button changes to Close Tunnel.)

Advanced IPSec Configuration

Note: The advanced IPSec settings apply *only* to the associated IPSec configuration (phase 2 settings).

➢ **To configure advanced IPSec settings:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name for which you want to configure the advanced settings (for example, Tunnel in the following figure). The IPSec pane displays.
2. In the IPSec pane, click the **Advanced** tab. The Advanced IPSec pane displays:

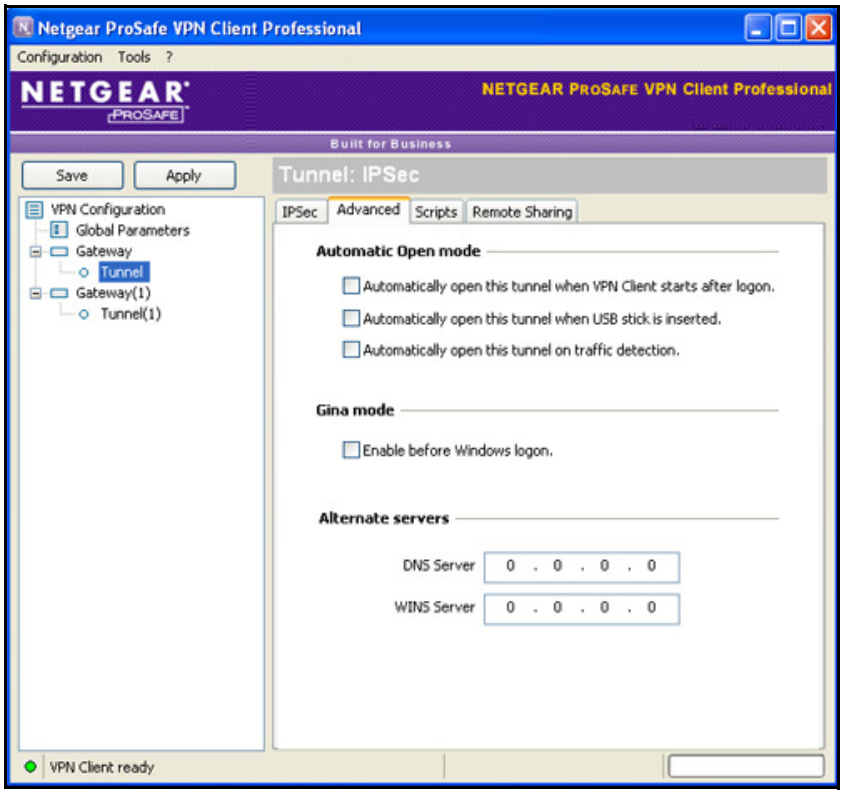


Figure 41.

3. Configure the settings as explained in the following table.

Figure 42. Advanced IPSec configuration settings (phase 2 settings)

Settings	Description
Automatic Open mode **Note:** When you select any of these check boxes, the VPN Client automatically opens the tunnel to which these advanced setting apply.	
Automatically open this tunnel when the VPN Client starts after login.	Select this check box to automatically open the tunnel when the VPN Client starts after you have logged in.
Automatically open this tunnel when USB stick is inserted.	Select this check box to automatically open the tunnel when you insert an external USB drive in to the computer. (For more information, see *USB Mode* on page 62). **Note:** This check box is disabled before Windows logon.

Figure 42. Advanced IPSec configuration settings (phase 2 settings) (continued)

Settings	Description
Automatically open this tunnel on traffic detection.	Select this check box to automatically open the tunnel when the VPN Client detects traffic.
Gina Mode	
Enable before Windows logon.	Select this check box to enable Gina mode, which is a mode that allows the tunnel to be used by Vista Credential Providers (also referred to as Gina mode on Windows 2000 and Windows XP) to process Windows logon. This mode can be useful when a corporate employee database is used for logon and the remote computer needs to connect to the corporate network before processing the Windows logon. For more information, see *Open a VPN Tunnel before Windows Logon* on page 37. **Note:** In Gina mode, the Scripts pane is disabled.
Alternate servers **Note:** When the Mode Config feature is enabled (see *Configure Advanced Authentication* on page 47), these fields are disabled. DNS server and WINS server addresses that are issued by the remote VPN gateway to the VPN Client are displayed in these fields.	
DNS Server	Enter the IP address of the DNS server of the remote LAN. The DNS server is used to resolve Intranet addressing while the tunnel is open. If Mode-Config is enabled, the DNS server address that is issued by the remote VPN gateway is displayed in this field.
WINS Server	Enter the IP address of the WINS server of the remote LAN. The WINS server is used to resolve intranet addressing while the tunnel is open. If Mode-Config is enabled, the WINS server address that is issued by the remote VPN gateway is displayed in this field.

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Script Configuration

This feature enables you to specify and execute scripts (including batches and applications) at each step of a tunnel connection for a variety of purposes, for example, to detect the current software release, to detect the database availability before launching a backup application, to configure the network, to detect whether or not a software application is running or a logon procedure is specified, and so on.

You can specify and execute several scripts for each step of a VPN tunnel opening and closing process:

- Before tunnel is opened
- After the tunnel is opened
- Before the tunnel closes
- After the tunnel is closed

➢ **To configure scripts:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name for which you want to configure the advanced settings (for example, Tunnel in the following figure). The IPSec pane displays.
2. In the IPSec pane, click the **Scripts** tab. The Scripts pane displays:

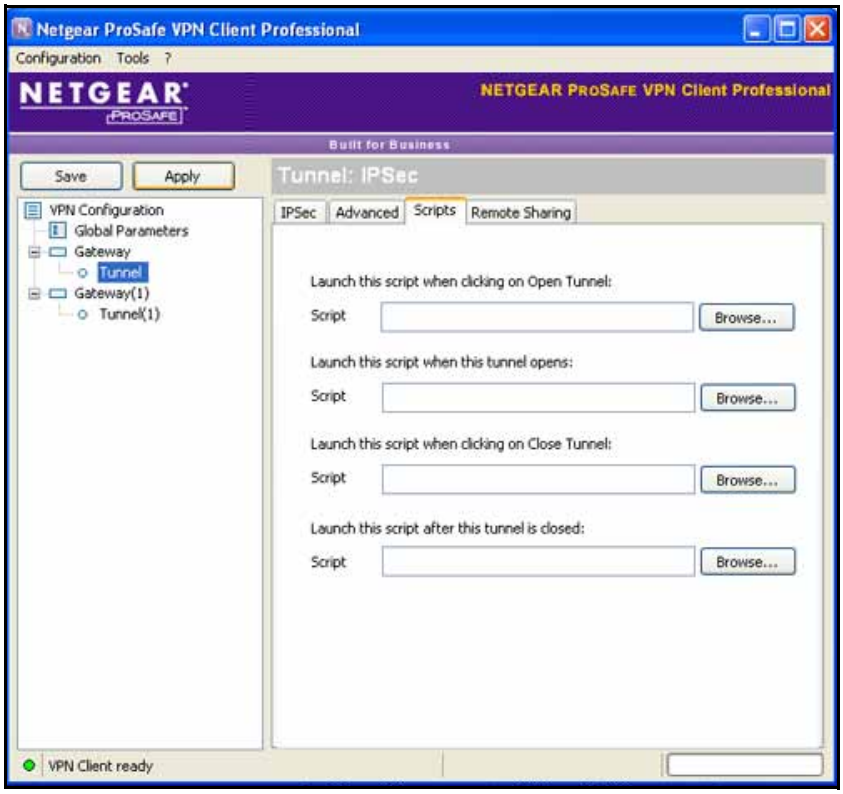


Figure 43.

3. Click **Browse** to navigate to a script file and open it. You can open up to four script files in the Scripts pane:
   - Launch this script when clicking on Open Tunnel.
   - Launch this script when this tunnel opens.
   - Launch this script when clicking on Close Tunnel.
   - Launch this script after this tunnel is closed.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Remote Sharing

This feature enables you to specify remote computers that you can connect to for desktop sharing after the VPN tunnel has been established.

➢ **To add a computer for remote sharing:**

1. In the tree list pane of the Configuration Panel screen, click the IPSec configuration name for which you want to configure the advanced settings (for example, Tunnel in the following figure). The IPSec pane displays.
2. In the IPSec pane, click the **Remote Sharing** tab. The Remote Sharing pane displays:

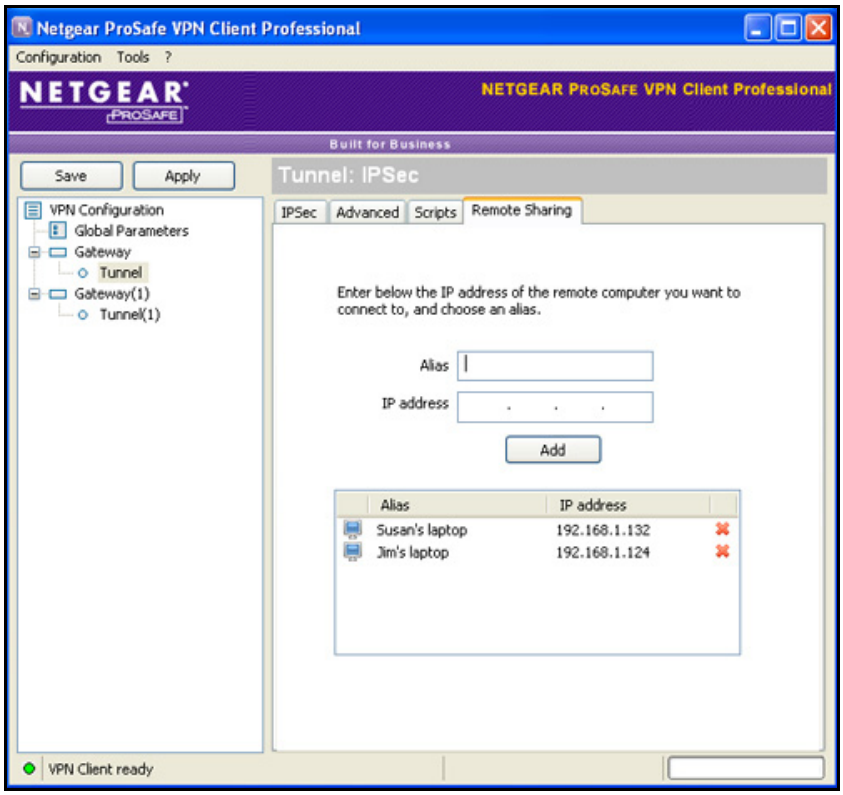


Figure 44.

3. In the Alias field, enter a name for the remote computer.
4. In the IP address field, enter the IP address for the remote computer. This needs to be an IP address in the subnet or IP range of the remote LAN.
5. Click **Add** to add the computer to the table.

After you have defined a remote computer, you can connect to it from the system tray menu. The VPN tunnel with which the remote computer is associated opens automatically.

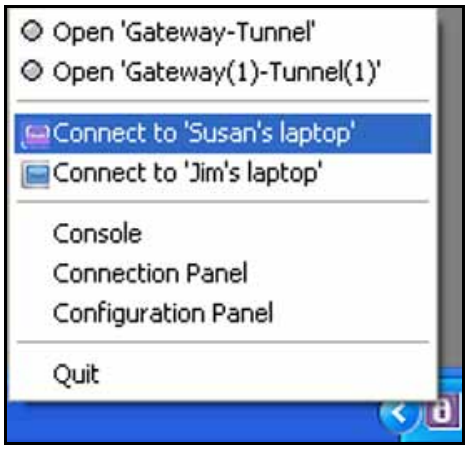


Figure 45.

Global Parameters

Global parameters are generic settings that apply to all VPN tunnels that you create.

➢ **To configure global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

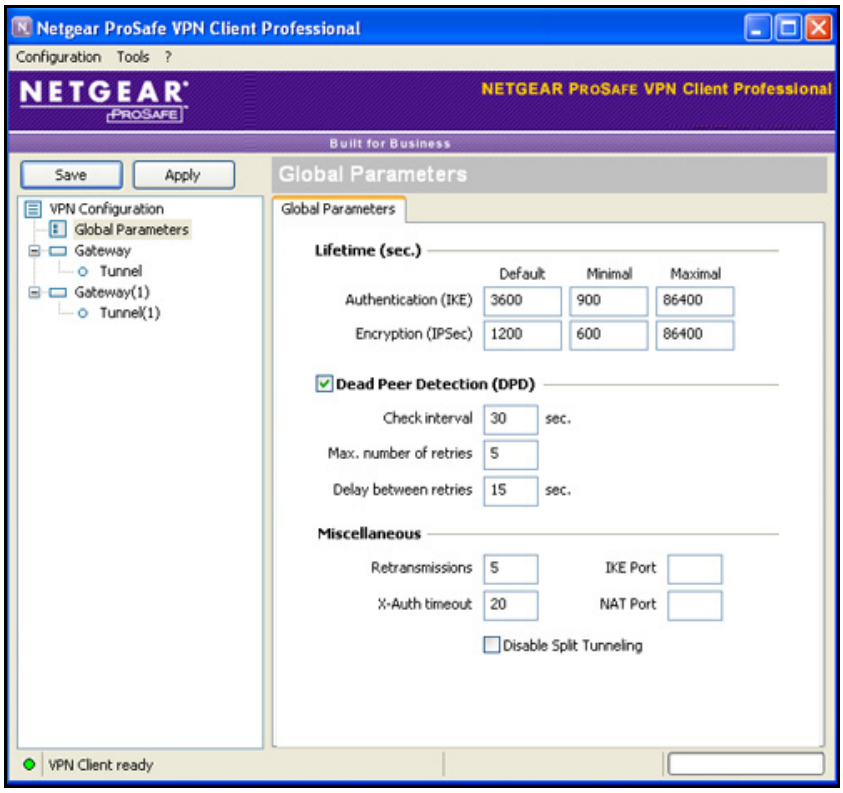


Figure 46.

2. Configure the settings as explained in the following table.

Table 7. Global parameters

Setting		Description
Lifetime (sec.)		
Authentication (IKE)	Default	Enter the default lifetime for IKE rekeying. The default is 3600 sec.
	Minimal	Enter the minimum lifetime for IKE rekeying. The default is 900 sec.
	Maximal	Enter the maximum lifetime for IKE rekeying. The default is 86400 sec.
Encryption (IPSec)	Default	Enter the default lifetime for IPSec rekeying. The default is 1200 sec.
	Minimal	Enter the minimum lifetime for IPSec rekeying. The default is 600 sec.
	Maximal	Enter the maximum lifetime for IPSec rekeying. The default is 86400 sec.
Dead Peer Detection (DPD) DPD is an Internet Key Exchange (IKE) extension (RFC3706) for detecting a dead IKE peer. The Dead Peer Detection (DPD) check box is enabled by default; if you want to disable DPD, clear the check box. The IPSec VPN Client uses DPD under the following circumstances: • To detect a dead peer and to delete the associated open SA in the VPN Client. • To restart IKE negotiations with an alternate gateway, if you have configured one (see *Advanced IPSec Configuration* on page 55).		
Check interval (sec.)		Enter the interval between DPD messages. The default is 30 sec.
Max. number of retries		Enter the number of times that DPD messages are sent when no reply is received from the peer. The default number is 5 times.
Delay between retries (sec.)		Enter the interval between DPD messages when no reply is received from the peer. The default is 15 sec.
Miscellaneous		
Retransmissions		Enter the number of times that a message should be retransmitted before the attempts are stopped. The default number is 5 times.
X-Auth timeout		Enter the time that is allowed to users to enter their XAUTH credentials. The default is 20 sec.
IKE Port		Enter the default UDP port that is used in the IKE negotiation during the authentication phase. The default port is 500 (which is not displayed in the IKE Port field). **Note:** Some firewalls do not allow IKE port 500, or outgoing traffic on port 500 might not be allowed. If you change the IKE port number, the remote gateway must be able to reroute the incoming traffic that is associated with a port other than IKE port 500.

Table 7. Global parameters (continued)

Setting	Description
NAT Port	Enter the default NAT port that is used during the IPSec negotiation. The default port is 4500 (which is not displayed in the NAT Port field). **Note:** Some firewalls do not allow NAT port 4500, or outgoing traffic on port 4500 might not be allowed. If you change the NAT port number, the remote gateway must be able to reroute the incoming traffic that is associated with a port other than NAT port 4500.
Disable Split Tunneling	Select this check box to limit traffic to encrypted traffic and force all traffic to go through the VPN tunnel.

3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

USB Mode

The VPN Client lets you save VPN configurations and VPN security elements such as preshared keys and certificates onto a USB drive to allow you to do the following:

- Limit a VPN configuration to a specific computer. VPN tunnels that are defined in the VPN configuration can be used only on a specific computer.
- Limit a VPN configuration to a specific USB drive. VPN tunnels that are defined in the VPN configuration can be used only with a specific USB drive.

After you have moved a VPN configuration and its security elements onto a USB drive and removed the USB drive, you then just need to insert the USB drive into a computer to automatically open the tunnels. When you remove the USB drive from the computer, all open tunnels are automatically closed.

Enable a New USB Drive with a VPN Configuration

You can enable a new USB drive by copying a VPN configuration and its security elements onto it in one of the following ways:

- From the main menu of the Configuration Panel screen, select **Configuration > Export**, and then copy the VPN configuration file onto the USB drive.
- Use the USB mode wizard.

➢ **To start the USB mode wizard and copy VPN configuration onto a USB drive:**

1. From the main menu of the Configuration Panel screen, select **Configuration > Move to USB Drive**. The USB Mode Wizard 1/4 screen displays:

Figure 47.

If one or more USB drives are already inserted, the VPN Client detects and displays them. In the previous figure, drive F: is selected.

Note: If you insert a USB drive with a VPN configuration while the USB Mode Wizard 1/4 screen is displayed, and the VPN Client detects that the USB drive is the only one in the computer, the VPN Client automatically displays the next screen, USB Mode Wizard 2/4.

Note: If you insert a USB drive with a VPN configuration while another USB drive with another VPN configuration is already inserted, a warning message asks you to remove one of the USB drives.

---

2. Click **Next**. The USB Mode Wizard 2/4 screen displays:

Figure 48.

3. Select one of the following security options:
   - **With this computer only**. The VPN tunnels that are defined in the VPN configuration can be used only on this specific computer.
   - **On any computer**. The VPN tunnels that are defined in the VPN configuration can be used with this USB drive only, but on any computer.
4. As an optional step, protect the VPN configuration with a password that you need to enter in the Password field. Select the **Hide password** check box to make the passport invisible.

> ***Note:*** At this step in the wizard, if you remove the USB drive, the wizard automatically returns to the USB Mode Wizard 1/4 screen.

5. Click **Next**. The USB Mode Wizard 3/4 screen displays:

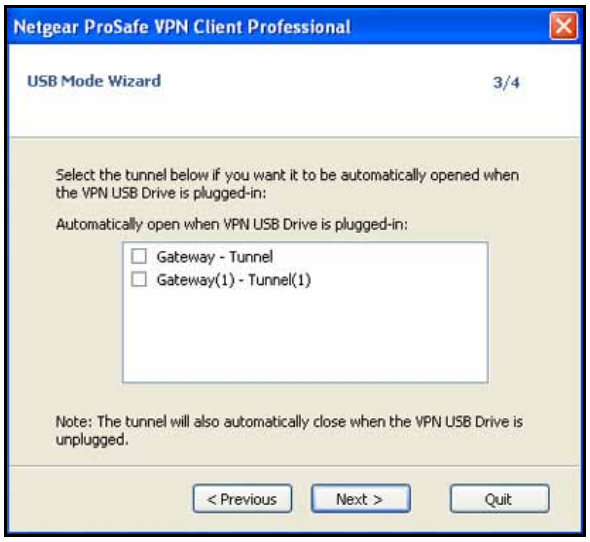


Figure 49.

6. Specify the tunnels that you want to be opened automatically by selecting the associated check boxes.

> ***Note:*** If there is only one tunnel configured, it is sufficient to select the **Automatically open this tunnel when USB stick is inserted** check box on the Advanced IPSec screen for the tunnel to be opened (see *Advanced IPSec Configuration* on page 55). If there is more than one tunnel configured, you need to select on the USB Mode Wizard 3/4 screen which tunnel or tunnels should be opened.

7. Click **Next**. USB Mode Wizard 4/4 screen displays. This screen is a summary screen.

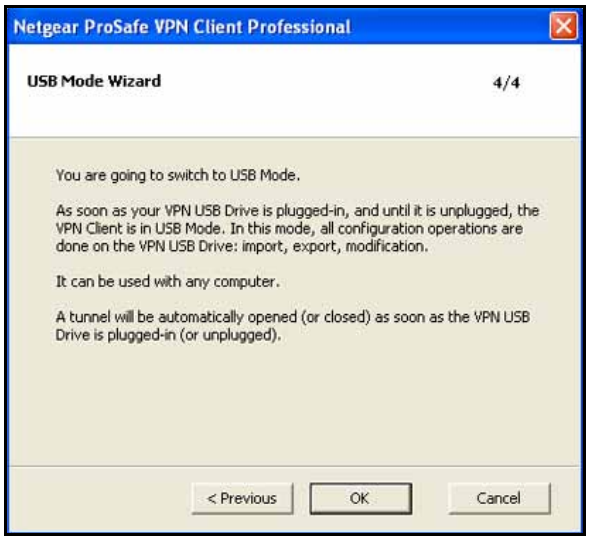


Figure 50.

8. Click **OK** to save the settings. The VPN configuration and its associated security information are now removed from the computer and copied onto the USB drive; the VPN Client is now functioning in USB mode.

Note: When you remove the USB drive from the computer, the VPN configuration is reset, that is, an empty configuration displays in the Configuration Panel screen. The next time that the VPN Client starts without the USB drive that contains the VPN configuration inserted, the VPN configuration is not present in the VPN Client.

Note: The VPN Client does not let you change the password or computer association that is on the USB drive. However, you can export the VPN configuration to a local disk, remove the USB drive, import the VPN configuration in the VPN Client, and start the USB mode wizard again to specify a new password or a new association with a computer. For information about importing and exporting, see *Import or Export a VPN Configuration* on page 76.

Automatic Opening of Tunnels

➢ **To enable a tunnel to be opened automatically:**

1. Select the **Automatically open this tunnel when USB stick is inserted** check box on the Advanced IPSec pane for the tunnel to be opened (see *Advanced IPSec Configuration* on page 55).
2. This step is required only if there is more than one tunnel configured:

   Select on the USB Mode Wizard 3/4 screen which tunnel or tunnels should be opened (see *USB Mode* on page 62).
3. Insert a USB drive that contains a VPN configuration.

   If you insert a USB drive without a VPN configuration, or if you do not insert a USB drive, the VPN Client starts in local mode and uses a VPN configuration that is available on the local disk.

Certificate Management

The VPN Client can use certificates from various sources:

- PEM format files
- PKCS#12 format file
- Personal Certificate Store
- USB token or smart card

The Certificate pane displays these certificate sources and lets you select a certificate for a particular tunnel. One certificate is bound to one tunnel. You can easily export the configuration to another computer.

Certificates can be stored on a USB token or smart card for which access is protected by a PIN code; the VPN Client uses these certificates dynamically while establishing a tunnel.

The VPN Client does not create certificates. You can create certificates by using third-party software such as Microsoft Certificates Server or OpenSSL (see *Appendix B, Generating Certificates With Microsoft Certificates Services and OpenSSL*) or purchase certificates from the Microsoft Certificate Store. You can store certificates on USB tokens and smart cards.

Assign Certificates

➢ **To assign a certificate to a tunnel:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to configure a certificate (for example, Gateway in the following figure). The Authentication pane displays (see *Figure 35* on page 46).
2. Select the **Certificate** radio button. The Certificate pane displays. (If the Certificate button was already selected in a previous configuration, just click the Certificate tab to display the Certificate pane.)

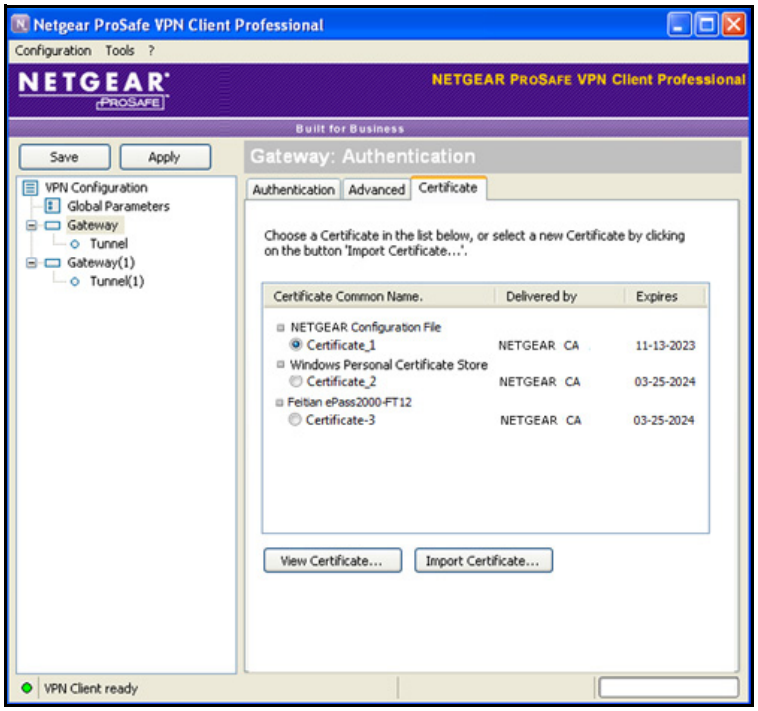


Figure 51.

The previous figure shows several sources from which you can select certificates. These sources are explained in the following table.

Table 8. Sources of certificates

Source	Description
NETGEAR configuration file	Certificates are located in the VPN configuration file that is used by the VPN Client. These certificates have been imported previously from another source such as a certificate file or the Microsoft Certificate Store.
Windows Personal Certificate Store	Certificates are located in the Personal Certificate Store. To be visible and usable, certificates need to be certified and in the correct location: • Certificates need to be certified by a certificate authority (CA) and the certificate status needs to be Ok (see also *Certificate Troubleshooting* on page 74). • Certificates need to be located in the Personal Certificate Store to represent the personal identity of the user attempting to connect to a corporate network.
USB token or smart card (such as Feitian ePass2000-FT21)	Certificates are located on one or more USB tokens and smart cards and are configured on the VPN Client. To use a certificate from a USB token or smart card, the USB token or smart card needs to be plugged into the computer. **Note:** When you remove the USB token or smart card from the computer, the certificate remains displayed on the Certificates pane but cannot be used until you plug the USB token or smart card back into the computer.

Note: For information about how to import a certificate, see *Import Certificates* on page 69.

3. Select one certificate from the list by selecting its associated radio button. You can select and assign only one certificate to a tunnel.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

View Certificate Details

➢ **To view the details of a certificate:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to view a certificate. The Authentication pane displays.
2. In the Authentication pane, click the **Certificate** tab. The Certificate pane displays.
3. Select a certificate from the certificate list.
4. Click **View Certificate**. The View Certificate screen displays (this can take up to 30 seconds), with the General tab selected by default.

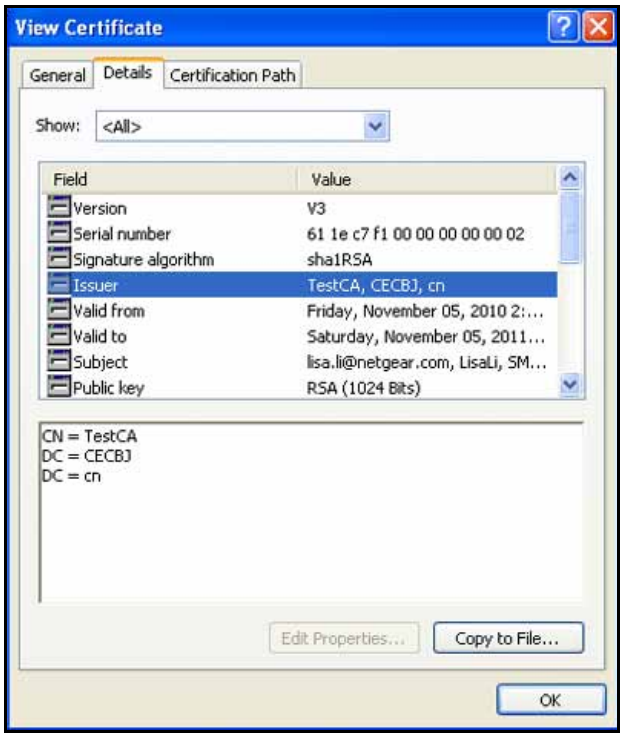


Figure 52.

You can click on the Details tab or Certification Path tab. When you click the Details tab, you can display the details of a certificate by clicking fields such as Issuer, Valid from, Valid to, Subject, and so on.

5. As an optional step, click **Copy to File** to open the Certificate Export Wizard that enables you to export the certificate to a file.
6. Click **OK** to close the View Certificate screen.

Import Certificates

You can import several certificates and assign each certificate to a different tunnel to enable the VPN Client to connect to various gateways that are part of different a Public Key Infrastructure (PKI).

You import and specify one PEM format and one P12 format per tunnel.

> ***Note:*** After you have imported a PEM or P12 certificate, the Local ID fields on the associated Advanced authentication pane are automatically set: the left field is set to Subject from X509 and the right field contains values from the certificate. For more information, see *Configure Advanced Authentication* on page 47.

PEM Certificates

➢ **To import a PEM certificate in a tunnel configuration:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to import a certificate. The Authentication pane displays.
2. In the Authentication pane, click the **Certificate** tab. The Certificate pane displays.
3. Click **Import Certificate**. The Import Certificate screen displays:

Figure 53.

4. Select the **PEM Format** radio button.
5. Click **Next**. The (PEM) Import Certificate screen displays:

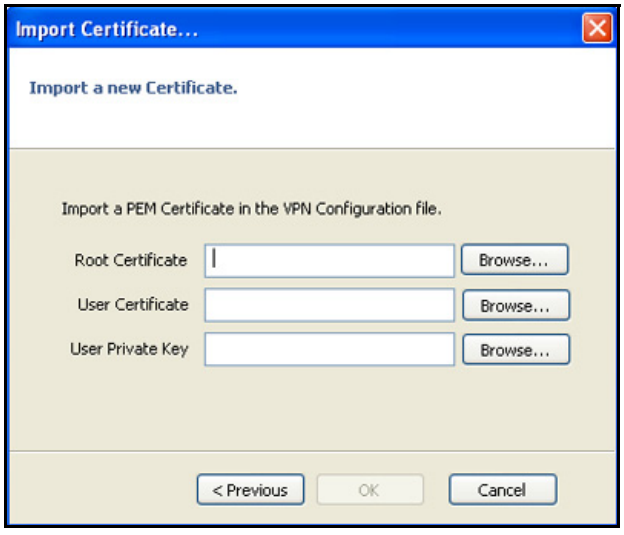


Figure 54.

6. Import the three PEM certificate files:
   - Next to the Root Certificate field, click **Browse**. Locate the root certificate file that you want to import. This file has either a .pem or a .crt extension.
   - Next to the User Certificate field, click **Browse**. Locate the user certificate file that you want to import. This file has either a .pem or a .crt extension.
   - Next to the User Private Key field, click **Browse**. Locate the user private key file that you want to import. This file has a .key extension.

> ***Note:*** A PEM certificate file that includes a user private key cannot not be encrypted or protected with a password.

7. Click **OK** to import the certificate. The Certificate pane now displays the imported certificate (see *Figure 51* on page 67).
8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

P12 Certificates

➢ **To import a P12 certificate in a tunnel configuration:**

1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to import a certificate. The Authentication pane displays.
2. In the Authentication pane, click the **Certificate** tab. The Certificate pane displays.
3. Click **Import Certificate**. The Import Certificate screen displays:

Figure 55.

4. Select the **P12 Format** radio button.

5. Click **Next**. The (P12) Import Certificate screen displays:

Figure 56.

6. Click **Browse**, and then locate and open the certificate file that you want to import. This file can have either a .p12 or a .pfx extension.
7. Click **OK** to import the certificate. The PKCS12 password file screen displays:

Figure 57.

8. Enter the password, and click **OK**. The Certificate pane now displays the imported certificate (see *Figure 51* on page 67).
9. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Use Certificates from USB Tokens and Smart Cards

The VPN Client can read certificates from USB tokens and smart cards. Smart cards can contain X509 certificates that can be protected by a PIN code.

➢ **To configure a tunnel with a certificate from a USB token or smart card:**

1. Insert a USB token or smart card into the computer.
2. If requested as part of USB token or smart card reader identification process, enter the PIN code and click **OK**.
1. In the tree list pane of the Configuration Panel screen, click the authentication phase name for which you want to use the certificate from the USB token or smart card. The Authentication pane displays.
2. In the Authentication pane, click the **Certificate** tab. The Certificate pane displays:

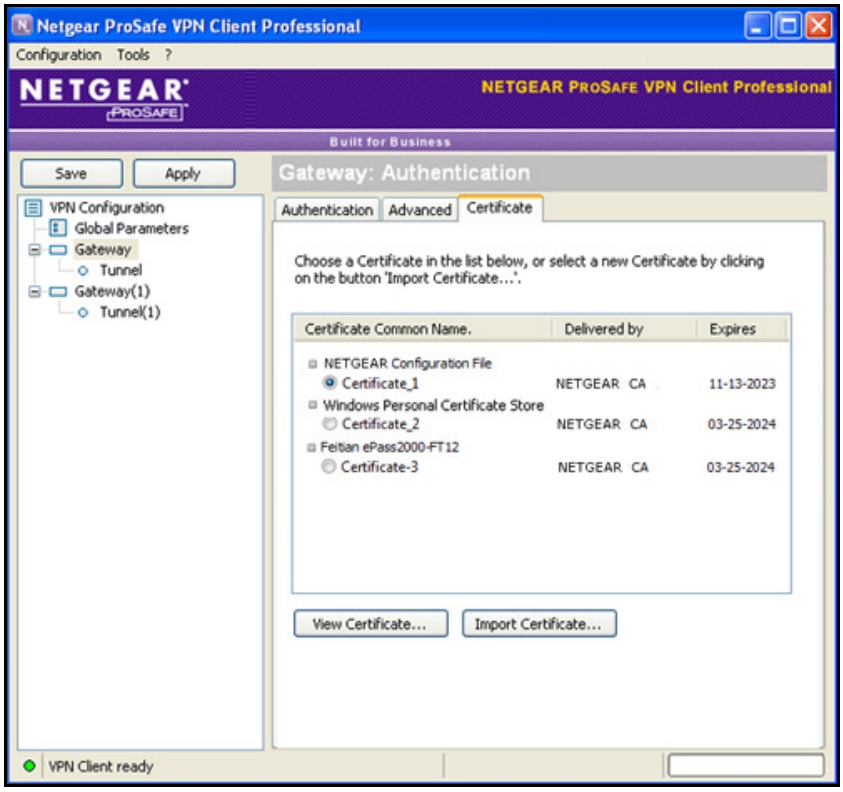


Figure 58.

The certificates from the USB token or smart card have been automatically imported and display in the certificates list.

3. Select a certificate by selecting its radio button.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Open a Tunnel with Certificates from a USB Token or Smart Card

When you have configured a tunnel to use a certificate from a USB token or smart card, you need to enter the PIN code that is associated with the USB token or smart card each time that the tunnel is opened (except for automatic VPN renegotiations).

➢ **To open a tunnel with a certificates from a USB token or smart card:**

1. Ensure that either the smart card reader is inserted in the computer and contains a smart card or the USB token is inserted in the computer.
2. Enter the PIN code that is associated with the USB token or smart card.
3. Right-click the system tray icon, and select **Open '*<gateway name-tunnel name>*'**.

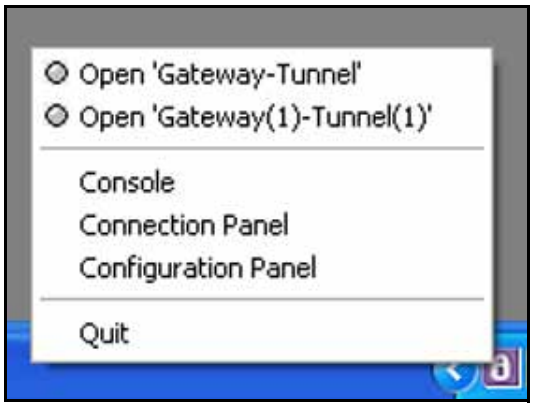


Figure 59.

Certificate Troubleshooting

Troubleshooting USB Tokens and Smart Cards

When an error occurs while you use a USB token or smart card, a small warning icon displays next to the token name. Click this warning icon to open a popup screen that provides more information about the error. One of the following errors might occur:

- **Error**: Token not found: previously plugged in but not at this time.

  Resolution: Reinsert the USB token or smart card.

- **Error**: Token found but no middleware to access it (often required when using smart card readers).

  Resolution: Install the software (middleware) that enables your computer to read the smart card, and restart the computer.

- **Error**: Token and store found but no certificate found.

  Resolution: Ensure that the certificate is located in the Personal Certificate Store to represent the personal identity of the user.

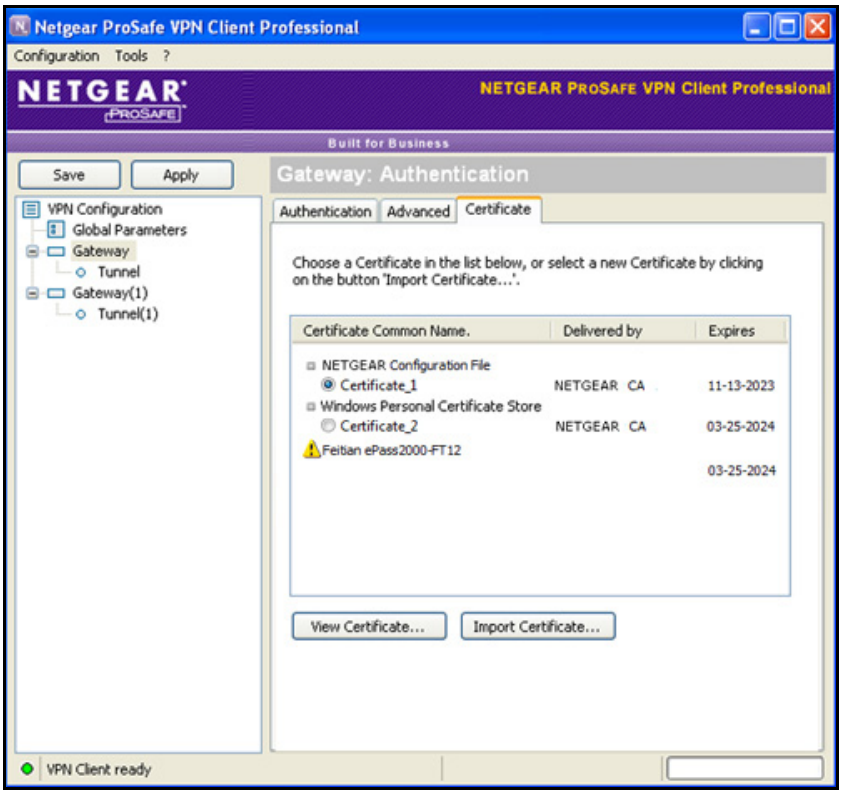


Figure 60.

Troubleshooting the Personal Certificate Store

To prevent errors, ensure the following:

- Certificates need to be certified by a certificate authority (CA), and the certificate status must be Ok.
- Certificates need to be located in the Personal Certificate Store to represent the personal identity of the user.

Windows provides a Certificate Management tool that you can use to troubleshoot certificate issues. To open this tool, select **Start > Run > certmgr.msc**.

VPN Configuration Management

Import or Export a VPN Configuration

The VPN Client can import or export a VPN configuration. This capability would typically be used by a network administrator to prepare a configuration and deliver it to other users.

➢ **To import a VPN configuration:**

1. From the main menu on the Configuration Panel screen, select **Configuration > Import**.
2. Navigate to the location of the VPN configuration file that you want to import, and click **Open**. An Information screens displays:

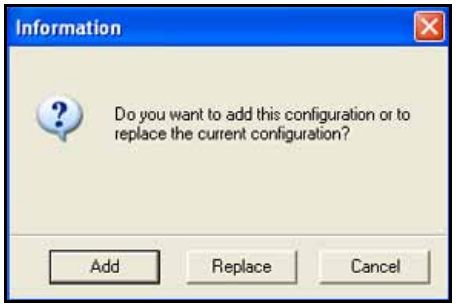


Figure 61.

3. Select one of the following buttons:
   - **Add**. Adds the imported VPN configuration to the existing VPN configuration.
   - **Replace**. Replaces the existing VPN configuration with the imported VPN configuration.

The imported VPN configuration displays in the tree list pane of the Configuration Panel screen.

Note: When you import a VPN configuration while the VPN Client is functioning in USB mode with a USB drive inserted in the computer, the file is automatically saved on the USB drive. If the VPN Client is functioning in USB mode but no USB drive is inserted in the computer, you cannot import or export a VPN configuration.

Note: For information about how to use the command-line interface (CLI) to import a VPN configuration file, see the following section and *Import, Export, Add, or Replace the VPN Configuration* on page 88.

➢ **To export a VPN configuration:**

1. From the main menu on the Configuration Panel screen, select **Configuration > Export**. The Export Protection screen displays:

Figure 62.

As a security measure, you have the option to specify a password for the exported file.

2. Select one of the following radio buttons:
   - **Don't protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. Enter a password in the field. The VPN configuration file can be opened with this password.
3. Click **OK**.
4. Navigate to the location where you want to save the VPN configuration file, and click **Save**. An exported VPN configuration file has a .tgb extension.

You can now forward the VPN configuration or double-click the VPN configuration shortcut icon to start the VPN Client.

Note: When you export authentication settings (phase 1 settings), the associated IPSec configurations (phase 2 settings) are also exported, including certificates that might have been defined in the IPSec configuration, and global parameters.

Merge VPN Configurations

You can import one or several tunnels into an existing VPN configuration. This capability would typically be used by a network administrator to merge a new VPN configuration with new gateways into an existing VPN configuration and deliver it to other users.

➢ **To merge VPN configurations, use one of the following three methods:**

- From the main menu on the Configuration Panel screen, select **Configuration > Import**, and then select **Add** instead of **Replace**, as explained in the procedure *To import a VPN configuration:* on page 76.
- Drag and drop a new VPN configuration onto the tree list pane of the Configuration Panel screen, and then select **Add** instead of **Replace**.
- Import a new VPN configuration using the CLI by entering **`[path]\vpnconf.exe /add:[file.tgb]`**, in which **`[path]`** is the VPN Client installation directory, and **`[file.tgb]`** is the VPN configuration file. This command does not process relative paths such as **`..\..\file.tgb`**. For more information, see *Import, Export, Add, or Replace the VPN Configuration* on page 88.

Regardless of how you import a VPN configuration, the following rules apply:

- If at least one tunnel is already configured before you import and add the VPN configuration, global parameters are *not* imported.
- If you import and replace the VPN configuration, or if no tunnel is configured when you import and add the VPN configuration, global parameters *are* imported.
- If there is a tunnel name conflict between an existing and an imported VPN configuration, the VPN Client automatically resolves this conflict by adding an increment between brackets—for example, tunnel_office(1)—to the imported tunnel name.

Split a VPN Configuration

You can export a single tunnel configuration from an existing VPN configuration. This capability would typically be used by a network administrator to split an existing large VPN configuration into a smaller VPN configuration and deliver it to other users.

➢ **To export a single tunnel configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the IPSec configuration name for which you want to export the tunnel configuration (for example, Tunnel in the following figure), and select **Export**.

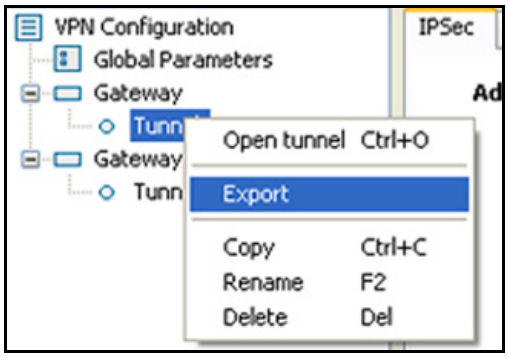


Figure 63.

The Export Protection screen displays:

Figure 64.

As a security measure, you have the option to specify a password for the exported file.

2. Select one of the following radio buttons:
   - **Don’t protect the exported VPN Configuration**.
   - **Protect the exported VPN Configuration**. Enter a password in the field. The VPN configuration file can be opened with this password.
3. Click **OK** to save the settings.
4. Navigate to the location where you want to save the VPN configuration file, and click **Save**. An exported VPN configuration file has a .tgb extension.

You can now forward the VPN configuration or double-click the VPN configuration shortcut icon to start the VPN Client.

Note: When you export an IPSec configuration (phase 2 settings), the associated authentication settings (phase 1 settings) are also exported, including certificates that might have been defined in the authentication settings, and global parameters.

Embed Your Own VPN Configuration in a VPN Client Software Setup

You can include a preconfigured VPN configuration in the VPN Client software setup. This capability would typically be used by a network administrator to deploy a preconfigured VPN Client in a single package to other users. For information, see *Embedded VPN Configuration* on page 81.

Demo VPN Configuration

The VPN Client software setup embeds a demo VPN configuration. This demo VPN configuration enables you to open a tunnel to a demo server after the VPN Client is installed.

Using the demo VPN configuration and demo server, you can check for testing and debugging purposes if a tunnel can be opened from your computer to an operational remote network. You can also find this demo VPN configuration at *http://www.thegreenbow.fr/doc/tgbvpn_demo.tgb*.

VPN Client Software Setup and Deployment

7

The VPN Client is designed to be easily deployed and managed. It implements several features that enable a network administrator to preconfigure the VPN Client software setup before deployment, to remotely install or upgrade the VPN Client, and to centrally manage VPN configurations. This chapter includes the following sections:

- *Embedded VPN Configuration*
- *VPN Client Software Setup Commands*
- *Command-Line Interface Commands*
- *Support for ATR Codes (Using Smart Cards)*

Note: The information in this chapter is typically used by network administrators.

Note: Enter software setup commands and command-line interface (CLI) commands in a command screen.

Note: For more information about software setup and the CLI, see *Appendix A, VPN Client Software Setup Deployment and Command-Line Interface Guide*.

Embedded VPN Configuration

An unzipped VPN configuration .tgb file is embedded within the VPN Client software setup and is automatically imported by the VPN Client during its installation.

➢ **To create a VPN Client software setup with a VPN configuration:**

1. Create the VPN configuration that you want to embed in the software setup. You do this by exporting the VPN configuration (that is, a .tgb file) from a formerly installed VPN Client and by importing the VPN configuration into the software setup.
2. Create a silent software setup (see *Create a Silent VPN Client Software Setup* on page 126), or unzip the VPN Client software setup file (NETGEARVPNClientPro_Setup.exe).
3. Add the VPN configuration file (that is, the .tgb file) to the unzipped setup directory.
4. Deploy the package to the user. The VPN configuration will be used during the software setup.

Note: The software setup cannot import and process an encrypted (protected) VPN configuration. When you create your VPN configuration, make sure that it is exported without being encrypted or without being protected with a password.

VPN Client Software Setup Commands

Several commands are available for the VPN Client software setup. These commands are described in the following sections:

- *Software Setup for GUI Mode* on page 83
- *Software Setup for GUI Mode with Access Control* on page 83
- *Software Setup for System Tray Menu Items* on page 84
- *Other Software Setup Options* on page 85

The following is an example of the syntax for a software setup:

```
NETGEARVPNClientPro_Setup.exe /S --license=0123456789ABCDEF0123 --activmail=
smith@smith.com
```

Note that you can use the following software setup commands only when the **/S** switch (silent mode installation, case-sensitive) is active:

```
--guidefs
--menuitem
--license|
--start
--activmail
--password
--autoactiv
--noactiv
--lang
--reboot
```

Software Setup for GUI Mode

➢ **To define the user interface appearance when the VPN Client starts:**

Enter the **`--guidefs=full`**, **`--guidefs=user`**, or **`--guidefs=hidden`** software setup command.

These are the options:

- **`full`**. The Configuration Panel screen is displayed. This is the default setting.
- **`user`**. The Connection Panel screen is displayed.
- **`hidden`**. Neither the Configuration Panel screen nor the Connection Panel screen is displayed. Only the system tray menu can be opened. Tunnels can be opened from the system tray menu.

The following figure shows the system tray menu after you have entered the **`--guidefs=hidden`** software setup command.

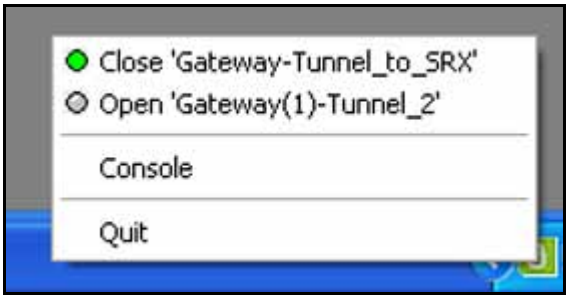


Figure 65.

Software Setup for GUI Mode with Access Control

➢ **To enable access control to the Configuration Panel screen with a password:**

Enter the **`--password=[password]`** software setup command, in which **`[password]`** is the specified password.

> ***Note:*** *Do not include the brackets in the software setup command.*

For more information, see *View Pane: Access Control and Hidden Interface* on page 27.

After implementation, you are asked for the password under the following circumstances:

- When you click or double-click the VPN system tray icon
- When you want to switch from the Connection Panel screen to the Configuration Panel screen

Figure 66.

The following is an example of the syntax for a software setup:

```
--guidefs=user --password=admin01
```

This example locks the VPN Client in the Connection Panel screen, while access to the Configuration Panel screen is protected with a password.

Software Setup for System Tray Menu Items

➢ **To specify the items of the system tray menu that you want to keep visible:**

Enter the **`--menuitem=[0...31]`** software setup command.

The value is a bit field:

1. Quit menu item displays.

2. Connection Panel menu item displays.

4. Console menu item displays.

5. Quit and Console menu items display.

16. Configuration Panel menu item displays.

31. All menu items display. This is the default setting.

The following is an example of the syntax for a software setup:

```
--menuitem=5
```

This example configures a system tray menu with the Quit and Console menu items.

Note: Tunnels are always shown in the system tray menu and can always be opened and closed from the system tray menu.

> ***Note:*** By default, --**guidefs=hidden** sets the system tray menu item list to Quit and Console (that is, the Connection Panel menu items are not visible). However, **--menuitem** overrides **--guidefs**. That means that when you enter **--guidefs=hidden --menuitem=1**, the system tray menu shows the Quit menu item only.

Other Software Setup Options

> ***Note:*** For more information about software setup commands, see *Software Setup Command Reference* on page 135.

> ***Note:*** Do not include the brackets in the software setup options.

You can enter the following commands in the software setup:

- **/S** to enable a silent uninstallation of an already installed version followed by a silent installation of a specified version (no dialogs are displayed during the uninstallation and installation). If there is no version installed, the uninstallation is ignored. **S** needs to be preceded by only one slash and is case-sensitive. The following is an example:

  ```
  NETGEARVPNClientPro_Setup.exe /S
  ```

- **/D=[install path]** in which **[install path]** is the path where the VPN Client is installed. **D** needs to be preceded by only one slash and is case-sensitive. Quotation marks are not allowed, even if there is a space in the path. You need to place this option at the end of the command line, as the last option, and you need to use it with the **/S** option (silent mode).
- **--license=[number]** to configure and automatically enter the license number, which consists of 20 or 24 hexadecimal characters.
- **--reboot=1** to automatically reboot the computer after a silent installation of the VPN Client.
- **--start=[1|2]** to configure the start mode for the VPN Client. These are the options:
  - **1**. The VPN Client starts after Windows login. This is the default setting.
  - **2**. You need to start the VPN Client manually.
- **--activmail=[activation_email]** to configure and automatically enter the email address that is used for activation confirmation. During the activation process, the field that is used to enter the email address is disabled.
- **--autoactiv=1** to activate the VPN Client automatically when the network is available during startup or when there is a request to open a tunnel. This option requires that the license number and activation email address have already been entered in a previous installation.

- **`--noactiv=1`** to prevent the Trial screen from displaying when the VPN Client starts until the trial period ends. A user other than the network administrator does not know about the trial period and the VPN Client is disabled at the end of the trial period. If a user attempts to launch the VPN Client after the end of trial period, the VPN Client starts and opens the Trial screen but the Evaluate button is disabled.
- **`--lang=[language code]`** to specify the language for the software setup and for the VPN Client. The available languages are shown in the following table.

Table 9. Available languages

ISO 639-2 Code	Language Code	English Name
AR	1025	Arabic
CZ	1029	Czech
DK	1030	Danish
DE	1031	German
EL	1032	Greek
EN	1033 (default)	English
ES	1034	Spanish
FI	1035	Finnish
FR	1036	French
HU	1038	Hungarian
IT	1040	Italian
JA	1041	Japanese
NL	1043	Dutch
NO	1044	Norwegian
PL	1045	Polish
RU	1049	Russian
TH	1054	Thai
TR	1055	Turkish
SL	1060	Slovenian
HI	1081	Hindi
ZH	2052	Chinese simplified
PT	2070	Portuguese
SR	2074	Serbian

The following is an example of a software setup that includes several options that are described in this section:

```
NETGEARVPNClientPro_Setup.exe /S --license=0123456789ABCDEF0123 --start=2
--activmail=smith@smith.com
```

Command-Line Interface Commands

> ***Note:*** For more information about command-line interface (CLI) commands, see *Command-Line Interface Command Reference* on page 139.

Several CLI commands are available to network administrators to adapt the VPN Client behavior to a specific environment and help integrate the VPN Client with other applications.

Open or Close VPN Tunnels

You can open or close a VPN tunnel through a CLI command. You can do this whether or not the VPN Client is running.

- **To open a VPN tunnel, enter the following CLI command:**

  `[path]\vpnconf.exe /open:[NamePhase1-NamePhase2]`

  in which

  `[path]` is the VPN Client installation directory.

  `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

  > ***Note:*** *Do not include the brackets in the CLI command.*

  If the specified tunnel is already open, the CLI command has no effect.

- **To close a VPN tunnel, enter the following CLI command:**

  `[path]\vpnconf.exe /close:[NamePhase1-NamePhase2]`

  in which

  `[path]` is the VPN Client installation directory.

  `[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

  > ***Note:*** *Do not include the brackets in the CLI command.*

  If the specified tunnel is already closed, the CLI command has no effect.

Note: The **open** and **close** commands are mutually exclusive.

Note: When you enter the **open** or **close** command, the user interface opens. This restriction will be removed in a future software release.

Stop the VPN Client

- **To stop the VPN Client, enter the following CLI command:**

  [path]\vpnconf.exe /stop in which **[path]** is the VPN Client installation directory.

  Note: Do not include the brackets in the CLI command.

  This CLI command closes all active tunnels.

  Use this CLI command, for example, in a script that starts the VPN Client after establishing a dial-up connection and closes it just before disconnecting the dial-up connection.

Import, Export, Add, or Replace the VPN Configuration

- **To enable the VPN Client to import a specific configuration file, enter the following CLI command:**

  [path]\vpnconf.exe /import:[ConfigFileName]

  in which

  [path] is the VPN Client installation directory,

  [ConfigFileName] is the VPN configuration file that has a .tgb extension.

  Note: Do not include the brackets in the CLI command.

  This CLI command does not handle relative paths such as **"..\..\file.tgb"**. Use double-quotes to specify paths that contain spaces.

  You can enter **/import:** whether or not the VPN Client is running. If the VPN Client is already running, it dynamically imports the new configuration and automatically applies it (that is, it restarts the IKE service). If the VPN Client is not running, it starts with the new configuration.

Instead of entering **/import:**, you can also enter one of the following commands to export, add, or replace a specific configuration file:

- **/importonce:** to import a VPN configuration file when the VPN Client is not running. This command is useful in installation scripts: it allows you to run a silent installation and to automatically import a VPN configuration file.
- **/export:** to export the current VPN configuration (including certificates) to the specified file and to start the VPN Client if it is not already running. This command also requires a password (for information, see the paragraph following this list).
- **/exportonce:** to export the current VPN configuration (including certificates) to the specified file. This command does not start the VPN Client if it is not running. This command also requires a password (for information, see the paragraph following this list).
- **/add:** to import a new VPN configuration into an existing VPN configuration and merge both into a single VPN configuration, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. You can use this command instead of the **/importonce:** command to import a VPN configuration file when the VPN Client is not running.
- **/replace:** to replace the current configuration with a new VPN configuration, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. You can use this command instead of the **/importonce:** command to import a VPN configuration file when the VPN Client is not running.

All six commands, **/import:**, **/importonce:**, **/export:**, **/exportonce:**, **/add:**, and **/replace:**, are mutually exclusive.

In addition, in combination with any of these commands, you can set a password by entering the **/pwd:[password]** CLI command. You need to place the **/pwd:[password]** CLI command *after* the other command that you are combining it with. The **/export:** and **/exportonce:** commands require a password.

Support for ATR Codes (Using Smart Cards)

Each new software release of the VPN Client includes the latest list of Answer to Reset (ATR) codes that are available from token and smart card vendors. Because new ATR codes appear every day, you have the option to manually add one or more new ATR codes to the VPN Client without waiting for a new software release.

Include the ATR code in an initialization file that you need to name vpnconf.ini. This file needs to be a text file and needs to be placed in the same installation folder as the tgbike.exe file.

The syntax for the vpnconf.ini file is as follows:

Table 10.

```
[3B:65:00:00:9C:02:02:07:02]
mask="FF:FF:00:00:FF:FF:FF:FF:FF"
scname="My token"
manufacturer="Token Manufacturer"
pkcs11DllName="pkcs11.dll"
registry="HKEY_LOCAL_MACHINE:SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\App
Paths\\TgbIke.exe:DllPath"

[3B:65:00:00:9C:02:02:07:03]
mask="FF:FF:00:00:FF:FF:FF:FF:FF"
scname="My token2"
manufacturer="Token Manufacturer"
pkcs11DllName="pkcs11.dll"
registry="HKEY_LOCAL_MACHINE:SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\App
Paths\\TgbIke.exe:DllPath"
```

The parameters are as follows:

Table 11. Parameters for the vpnconf.ini file

Parameter	Description
[atr]	Token ATR code. This the delimiter to separate several ATR codes.
mask	Token mask code.
scname	Token name.
manufacturer	Token manufacturer's name.
pkcs11DllName	PKCS#11 middleware file.

registry	Value in the registry that points to the complete path of the DLL.
	
	Note: If the PKCS#11 DLL (shown in the example as pkcs11.dll) is not in c:\windows\system32\, then the registry parameter must be set.
	
	The syntax is as follows:
	`HKEY_LOCAL_MACHINE:<registry key>:<value in the registry key>.`
	`For example, if a value "DllPath" with content:`
	`C:\Program Files\Netgear\Netgear VPN\pkcs11.dll`
	`is created in:`
	`HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\AppPaths\\TgbIke.exe,`
	`the registry line is:`
	`HKEY_LOCAL_MACHINE:SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\AppPaths\\TgbIke.exe:DllPath`

Configure the VPN Client with a NETGEAR Router

8

This chapter describes how to configure the VPN Client with a NETGEAR ProSafe SRX5308 VPN Firewall (in this chapter referred to as the SRX5308 VPN router). The chapter includes the following sections:

- *Introduction*
- *Sample VPN Network Topology*
- *Configure the SRX5308 VPN Router*
- *Configure the VPN Client*
- *Establish a VPN connection*

Introduction

In addition to the NETGEAR ProSafe SRX5308 VPN router, you can also apply the information in this chapter to the following NETGEAR ProSafe routers and ProSecure UTM appliances. The information in this chapter has been tested with the VPN Client firmware version 5.11 and the firmware releases that are listed in the following table.

Table 12. Tested firmware versions

Router	Firmware Version
FVS318N	4.0.1-67 or later
FVG318v2	2.1.3-29 or later
FVS336Gv2	3.0.7-79 or later
SRX5308	3.0.7-65 or later
UTM5	1.3.15.9 or later
UTM10	1.3.15.9 or later
UTM9S	2.1.0-3 or later
UTM25	1.3.15.9 or later
UTM50	1.3.15.9 or later

Sample VPN Network Topology

In the VPN network example that is shown in the following figure, the SRX5308 VPN router functions as a gateway for a main office. The Windows PC VPN Client is installed on a remote laptop that runs Windows 7 and that connects to the Internet through a DSL modem. The Windows PC VPN Client connects to the SRX5308 VPN router and establishes a secure IPSec VPN connection with the router so the laptop user can gain access to a file server or any other resources at the main office.

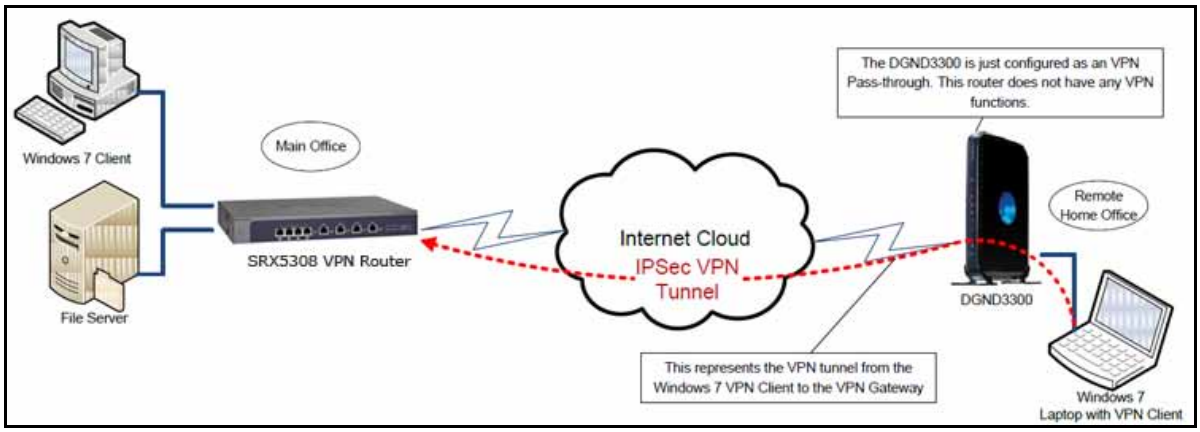


Figure 67.

The following table shows the IP addresses that are used in the VPN network example that is shown in the previous figure.

Main Office	Remote Home Office
Main office router: WAN IP: myrouter.dyndns.org or 10.200.13.18 SRX5308 IP address: 192.168.30.1 Subnet mask: 255.255.255.0 File server IP: 192.168.30.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.30.1 Windows 7 client IP: 192.168.30.3 Subnet mask: 255.255.255.0 Default gateway: 192.168.30.1	**Home office router:** DGND3300 IP address: 192.168.0.1 Subnet mask: 255.255.255.0 Windows 7 laptop with VPN Client: 192.168.0.2 Subnet mask: 255.255.255.0 Default gateway: 192.168.0.1 **VPN Client settings:** Pre-shared key: N3tg4ar12 Router identifier: srx_router.com VPN Client identifier: srx_client.com

Note: All the addresses in this chapter are for sample purposes only. You can adjust the settings and configuration to suit your network.

While you configure the SRX5308 VPN router, there is information that you add and that will later be used in the configuration of the VPN Client. This information is marked with a number in white font in a red circle (for example, ❸). You can print the following table to help you keep track of this information.

u	**Pre-shared key**	
v	**Remote identifier information**	
w	**Local identifier information**	
x	**Router's LAN network IP address**	
y	**Router's LAN network mask**	
z	**Router's WAN IP address**	

Configure the SRX5308 VPN Router

The router lets you to set up the VPN connection manually or with the integrated VPN Wizard, which is the easier and preferred method. The VPN Wizard configures the default settings and provides basic interoperability so that the VPN router can easily communicate with NETGEAR or third-party VPN devices.

Use the VPN Wizard to Configure a Client-to-Router VPN Connection

➢ **To use the VPN Wizard to set up a VPN connection between the VPN router and a client:**

1. Access the router's web management interface.
2. Select **VPN > IPSec VPN> VPN Wizard**. The VPN Wizard screen displays:

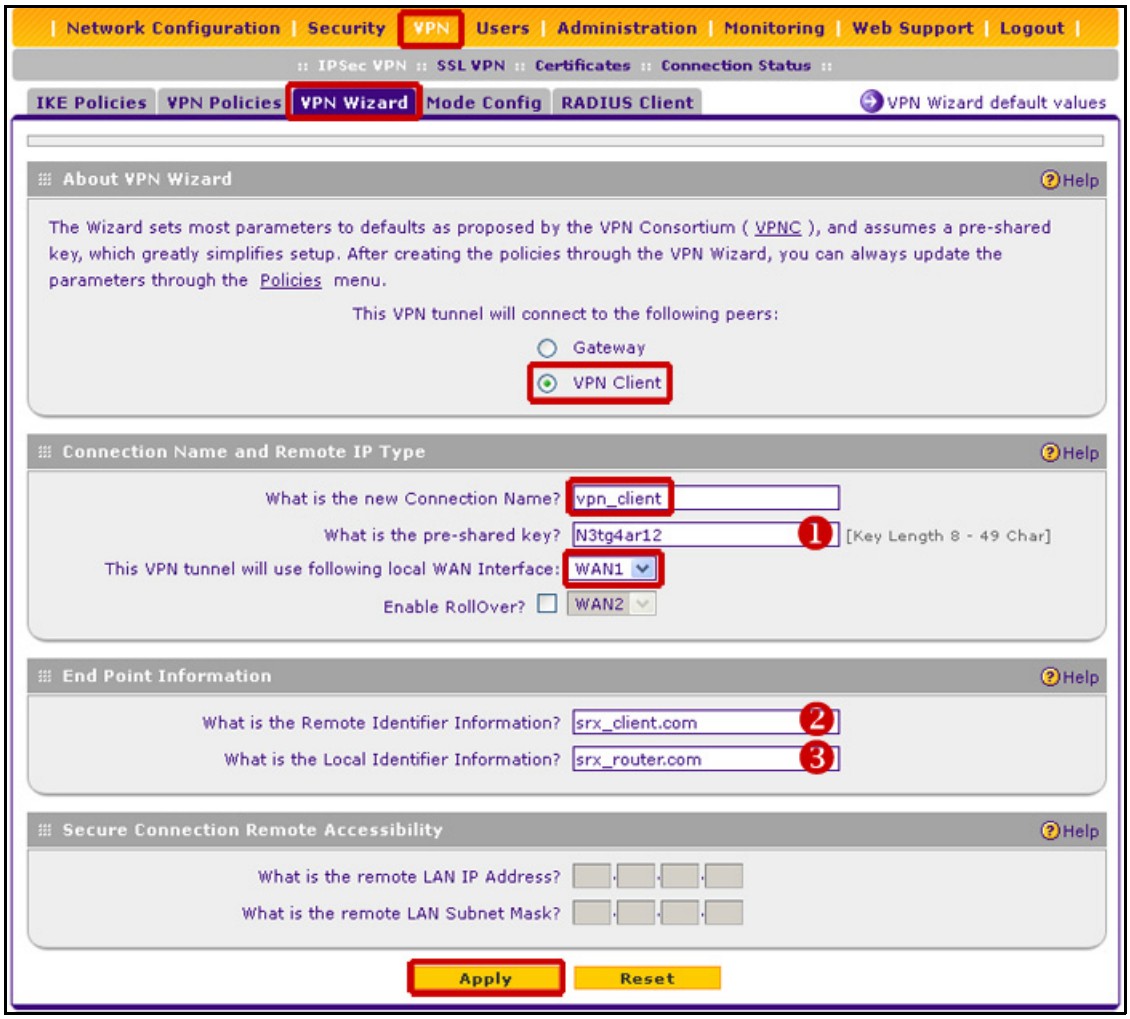


Figure 68.

3. Specify the settings that are explained in the following table.

Table 13. SRX5308 VPN Wizard screen settings

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **VPN Client** radio button.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter **vpn_client**.
What is the pre-shared key?	Enter the pre-shared key **N3tg4ar12**. 1 **Note:** This key must be at least 8 characters long and should not be easy to guess.

Table 13. SRX5308 VPN Wizard screen settings (continued)

Setting	Description
This VPN Tunnel will use the following local WAN Interface	Select **WAN1** from the pull-down menu. **Note:** This option is not available for platforms with a single WAN port.
End Point Information	
What is the Remote Identifier Information?	Enter **srx_client.com**. ❷ The default setting is srx_remote1.com.
What is the Local Identifier Information?	Enter **srx_router.com**. ❸ The default setting is srx_local1.com.

4. Click **Apply** to save the settings.
5. Review the policies by selecting **VPN > IPSec VPN > VPN Polices**. The VPN Policies screen displays. Take note of the local LAN IP address ❹ and subnet mask ❺, both of which you will later use in the configuration of the VPN Client.

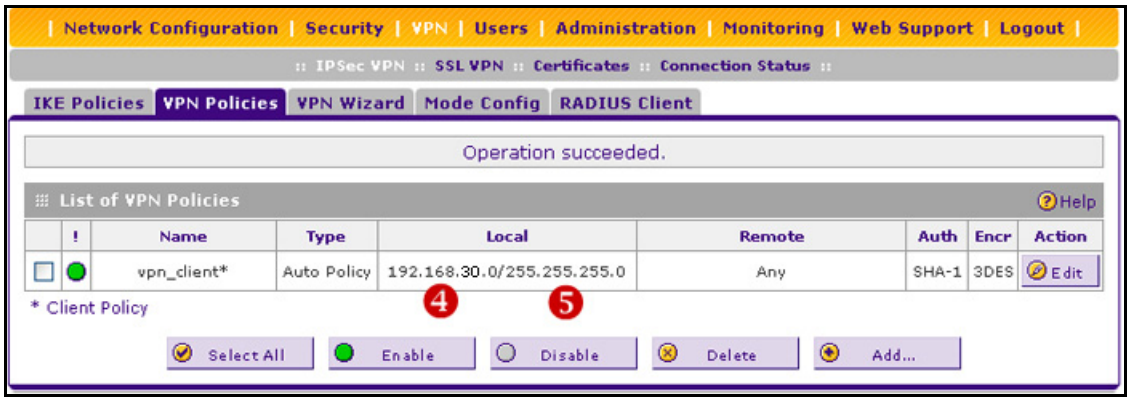


Figure 69.

6. Optional step. Review or edit the VPN policy. To edit the VPN policy:
   a. Disable the VPN policy by selecting the check box that is associated with the policy and then clicking **Disable**.
   b. Click **Edit** in the Action column of the VPN Policies screen to open the Edit VPN Policy screen.

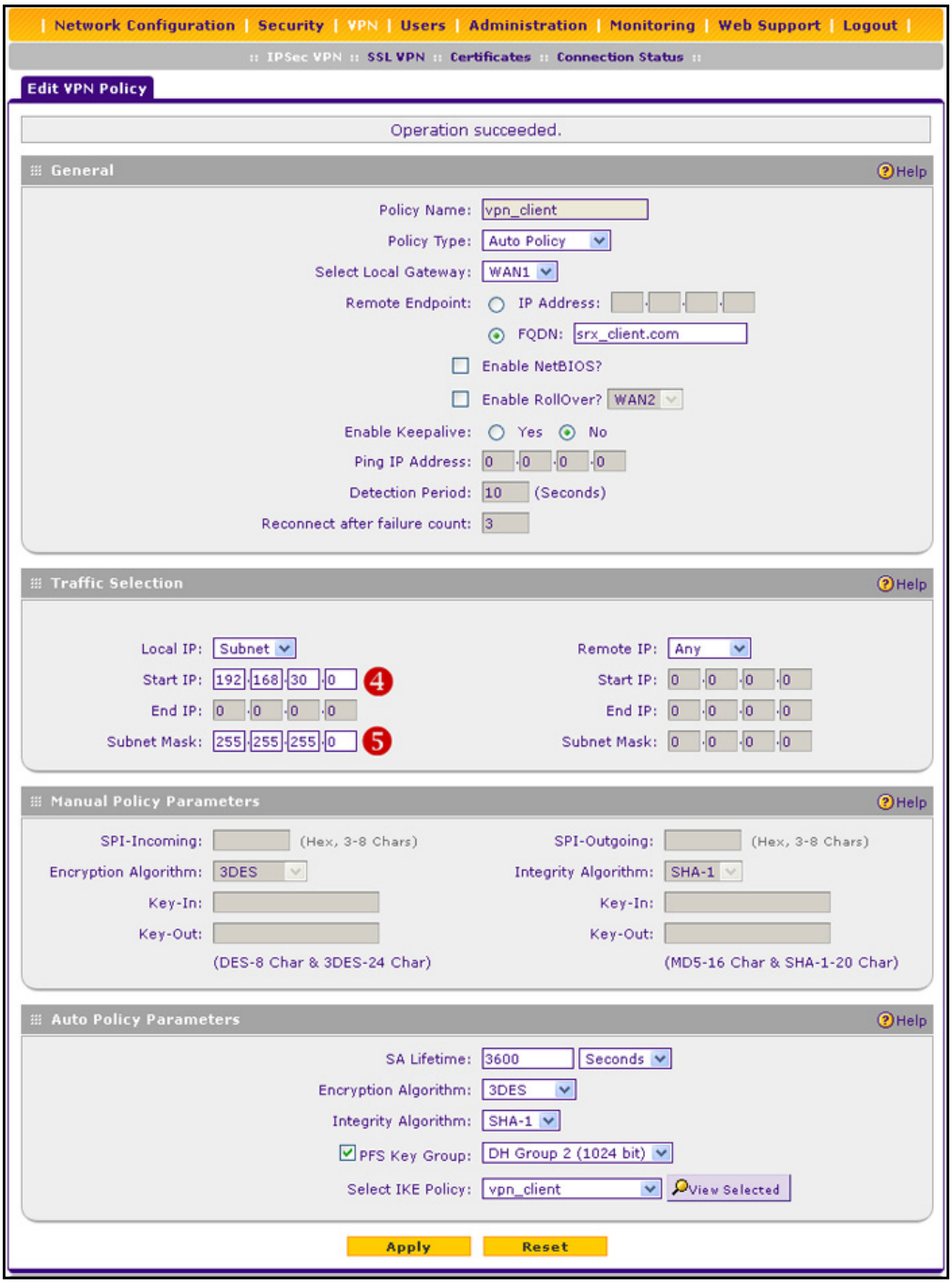


Figure 70.

c. Make your changes to the VPN policy, and click **Apply**. The VPN Policies screen displays again.

d. Reenable the VPN policy by selecting the check box that is associated with the policy and then clicking **Enable**.

7. Optional step. Review or edit the IKE policy. To edit the IKE policy:

   a. You cannot edit the IKE policy without disabling the associated VPN policy. On the VPN Policies screen, disable the associated VPN policy by selecting the check box that is associated with the policy and then clicking **Disable**.

   b. Click the **IKE Policies** tab. The IKE Policies screen displays. Take note of the remote ID ❷ and local ID ❸, both of which you will later use in the configuration of the VPN Client.

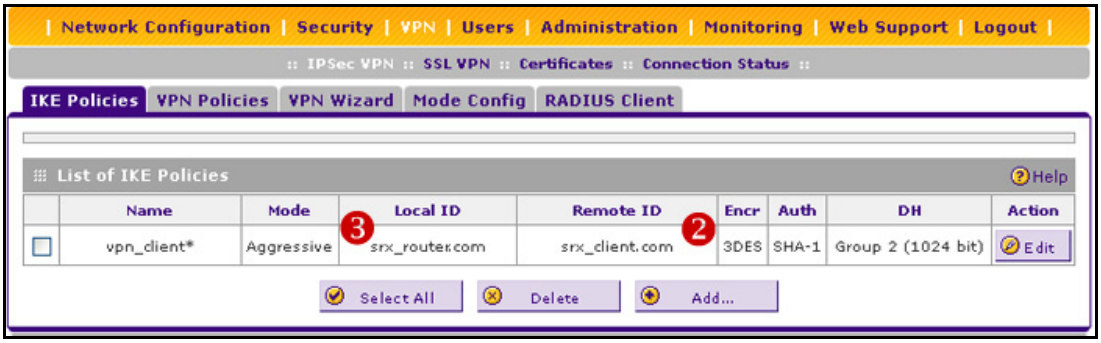


Figure 71.

   c. Click **Edit** in the Action column of the IKE Policies screen to open the Edit IKE Policy screen. Take note of the pre-shared key ❶, which you will later use in the configuration of the VPN Client.

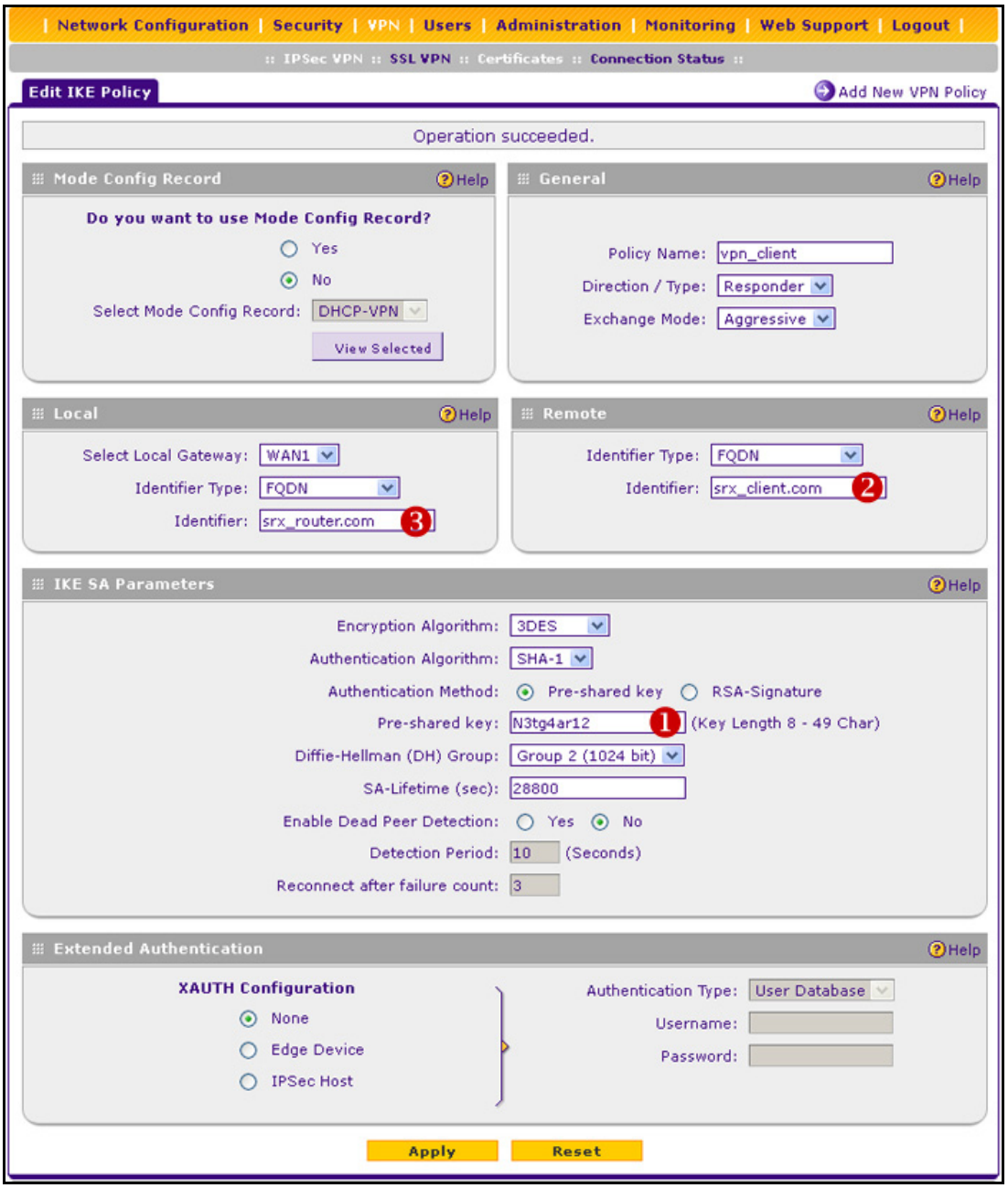


Figure 72.

d. Make your changes to the IKE policy, and click **Apply**. The IKE Policies screen displays again.

e. Reenable the VPN policy by clicking the **VPN Policies** tab to open the VPN Policies screen, selecting the check box that is associated with the policy, and then clicking **Enable**.

For information about how to configure the VPN Client, see *Configure the VPN Client* on page 103.

Manually Configure a Client-to-Router VPN Connection

To manually configure a VPN connection between the VPN router and a client, access the router's web management interface, create an IKE policy, and then create a VPN policy.

IKE Policy

➤ **To set up an IKE policy:**

1. Select **VPN > IPSec VPN > IKE Polices**. The IKE Policies screen displays.
2. Click **Add**. The Add IKE Policy screen displays:

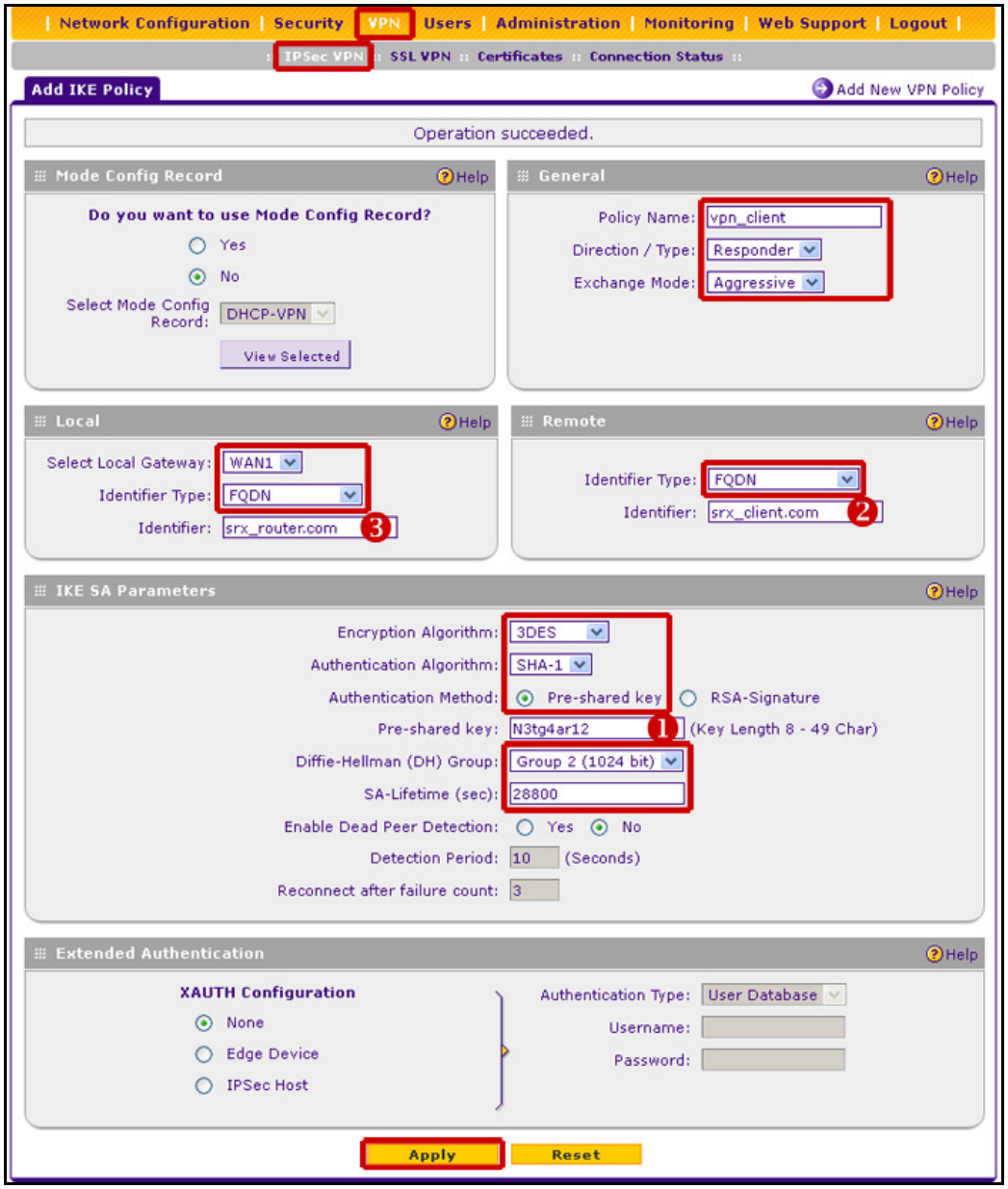


Figure 73.

3. Specify the settings that are explained in the following table.

Table 14. SRX5308 Add IKE Policy screen settings

Setting	Description
General	
Policy Name	Enter **vpn_client**.
Direction / Type	Select **Responder** from the drop-down list (the router will be responding to the client).
Exchange Mode	Select **Aggressive** (mode) from the drop-down list.
Local	
Select Local Gateway	Select **WAN1** from the pull-down menu. **Note:** This option is not available for platforms with a single WAN port.
Identifier Type	Select **FQDN** from the drop-down list.
Identifier	Enter **srx_router.com**. ❸
Remote	
Identifier Type	Select **FQDN** from the drop-down list.
Identifier	Enter **srx_client.com**. ❷
IKE SA Parameters	
Encryption Algorithm	Select **3DES** from the drop-down list.
Authentication Algorithm	Select **SHA-1** from the drop-down list.
Authentication Method	Select the **Pre-Shared Key** radio button.
Pre-shared key	Enter the pre-shared key **N3tg4ar12**. ❶ **Note:** This key needs to be at least 8 characters long and should not be easy to guess.
Diffie-Hellman (DH) Group	Select **Group 2 (1024bit)** from the drop-down list.
SA-Life Time (sec)	Enter **28800**.
Enable Dead Peer Detection	Select the **No** radio button. (This is the default setting.)
Extended Authentication	
Extended Authentication	Select the **No** radio button. (This is the default setting.)

4. Click **Apply**. The IKE Policies screen displays.

VPN Policy

➢ **To set up a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Polices**. The VPN Policies screen displays.
2. Click **Add**. The Add VPN Policy screen displays:

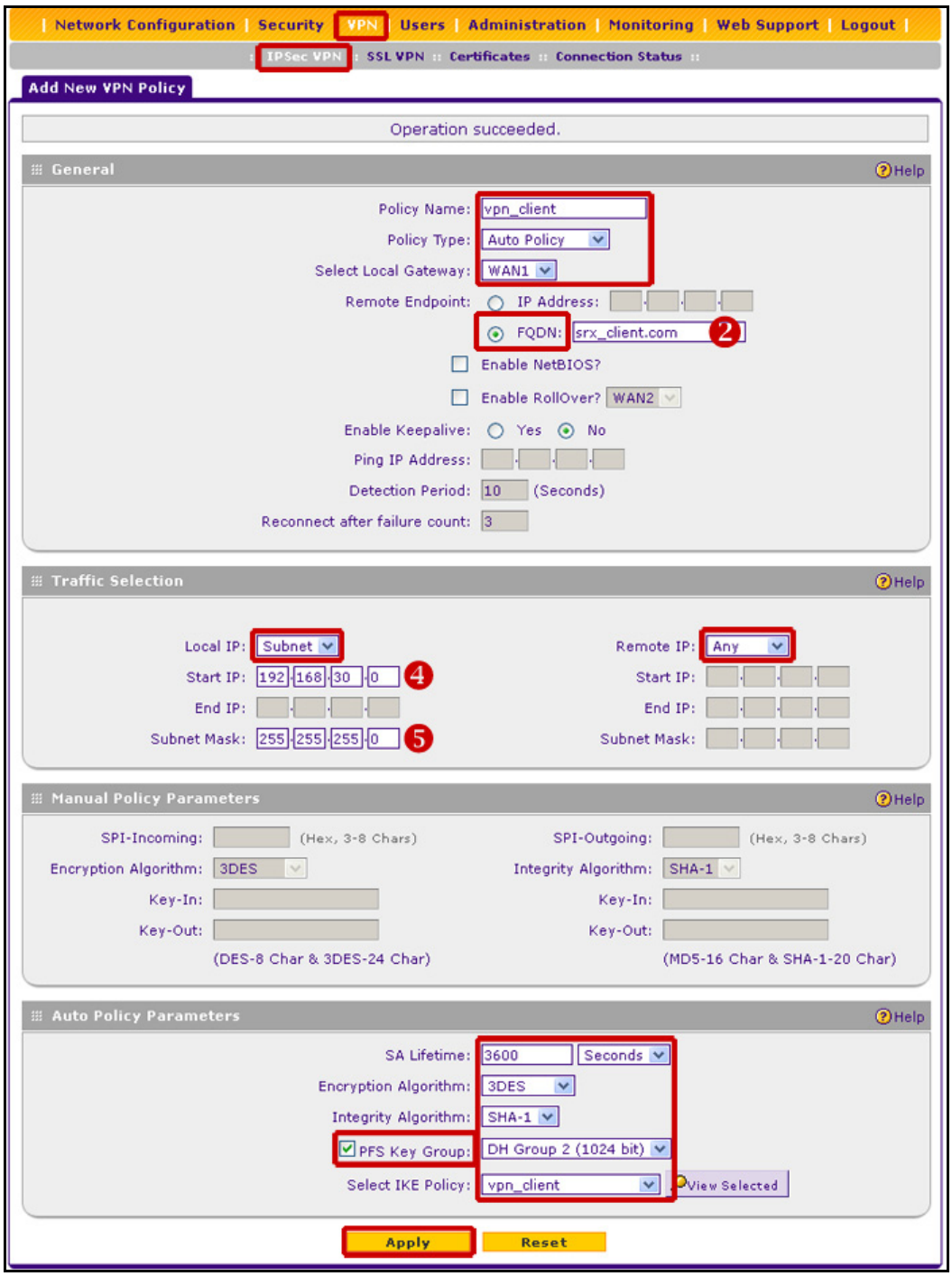


Figure 74.

3. Specify the settings that are explained in the following table.

Table 15. SRX5308 Add VPN Policy screen settings

Setting	Description
General	
Remote Endpoint	Enter **vpn_client**. (Keep the policy name the same as the IKE policy name.)
Policy Type	Select **Auto Policy** from the drop-down list.
Select Local Gateway	Select the **WAN1** radio button. **Note:** This option is not available for platforms with a single WAN port.
Remote Endpoint	Select the **FQDN** radio button, and enter **srx_client.com** in the field to the right. 2
Enable NetBIOS	Do not enable NetBIOS; leave this check box cleared. (This is the default setting.) **Note:** Because you are creating a client-to-router configuration, the remote IP addresses are likely unknown.
Enable RollOver	Do not enable rollover; leave this check box cleared. (This is the default setting.) **Note:** This option is not available for platforms with a single WAN port.
Enable Keepalive	Do not enable keep-alives; select the **No** radio button. (This is the default setting.)
Traffic Selection	
Local IP	Select **Subnet** from the drop-down list.
Start IP Address	Enter **192.168.30.0**. 4
Subnet Mask	Enter **255.255.255.0**. 5
Remote IP	Select **Any** from the drop-down list.
Auto Policy Parameters **Note:** If you select **Manual Policy** from the Policy Type drop-down list (see the General section on the screen), the Manual Policy Parameters section is enabled onscreen. Because you selected **Auto Policy**, the Auto Policy Parameters section is enabled.	
SA Lifetime	Enter **3600** and select **Seconds** from the drop-down list.
Encryption Algorithm	Select **3DES** from the drop-down list.
Integrity Algorithm	Select **SHA-1** from the drop-down list.

Table 15. SRX5308 Add VPN Policy screen settings (continued)

Setting	Description
PFS Key Group	Select the **PFS Key Group** check box, and then **DH Group 2 (1024 bit)** from the drop-down list.
Select IKE Policy	Select **vpn_client** from the drop-down list. This is the IKE policy that you created in the previous section.

4. Click **Apply**. The VPN Policies screen displays.

For information about how to configure the VPN Client, see the following section.

Configure the VPN Client

The VPN Client lets you to set up the VPN connection manually or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN Client can easily communicate with NETGEAR or third-party VPN devices. The Configuration Wizard does not let you enter the local and remote IDs, so you must manually enter this information.

Use the Configuration Wizard to Configure the VPN Client

Note: For another example of how to use the Configuration Wizard, see *Use the Configuration Wizard to Create a VPN Tunnel Connection* on page 41.

➢ **To use the Configuration Wizard to set up a VPN connection between the VPN Client and a router:**

1. Access the VPN Client's user interface, and from the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (screen 1 of 3) displays:

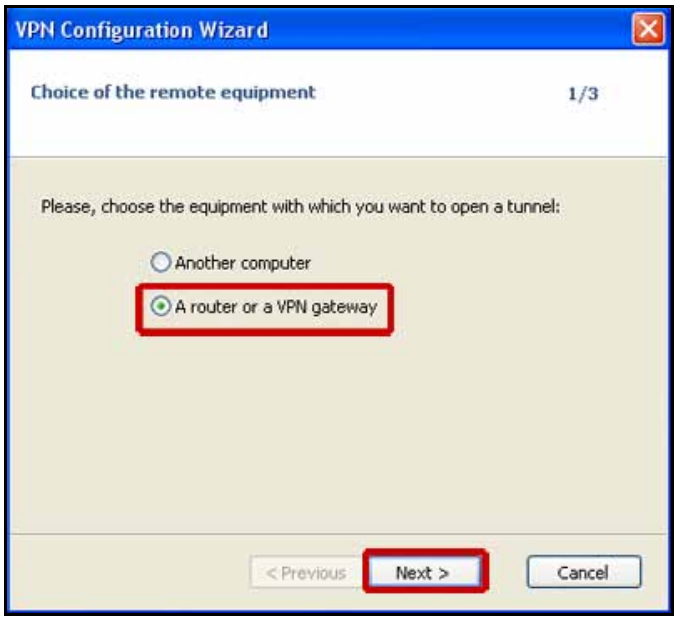


Figure 75.

2. Select the **A router or a VPN gateway** radio button, and click **Next**. The VPN tunnel parameters wizard screen (screen 2 of 3) displays:

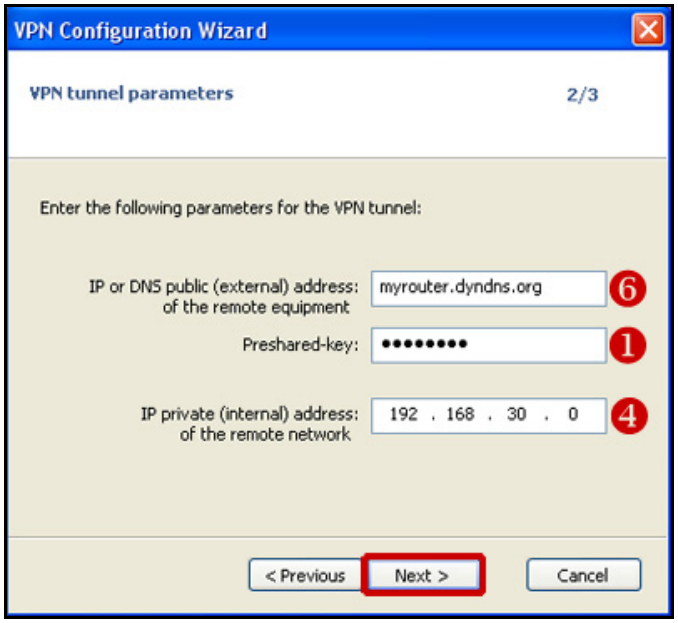


Figure 76.

3. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the VPN router. for example, **myrouter.dyndns.org** or **10.200.13.18**. ❻

- **Preshared key**. Enter **N3tg4ar12**, which is the preshared key that you already specified on the VPN router. ❶
- **IP private (internal) address of the remote network**. Enter **192.168.30.0**, which is the remote private IP address of the remote VPN router. This IP address enables communication with the entire 192.168.30.x subnet. ❹

4. Click **Next**. The Configuration Summary wizard screen (screen 3 of 3) displays:

Figure 77.

5. This screen is a summary screen of the new VPN configuration. Click **Finish**.
6. Specify the local and remote IDs:
   a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase). The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

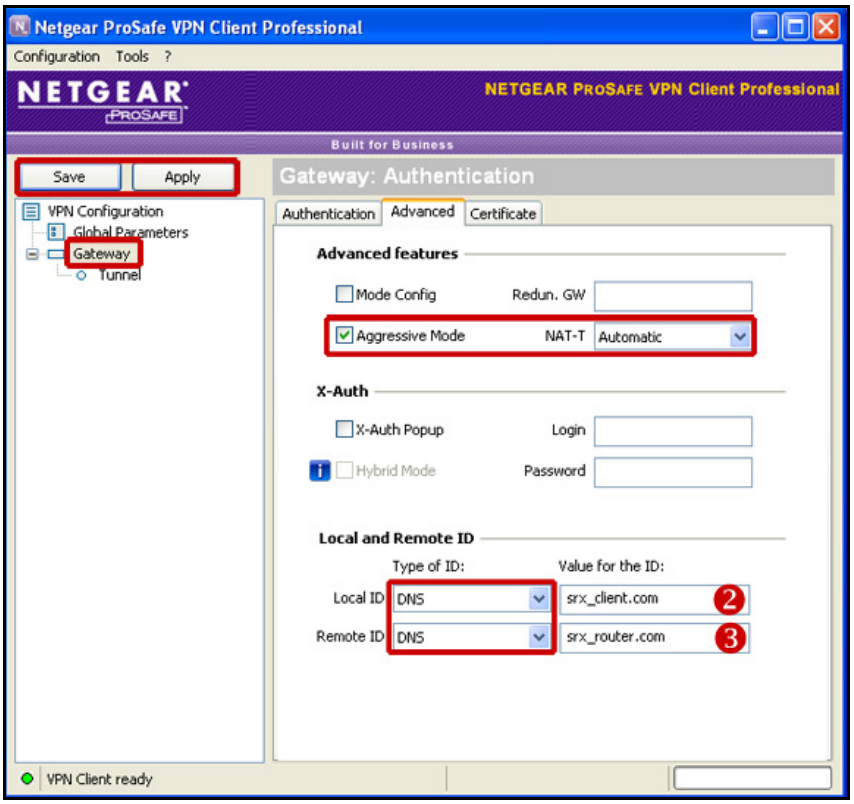


Figure 78.

b. Specify the settings that are explained in the following table.

Table 16. VPN Client advanced authentication settings

Setting	Description
Advanced Features	
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN router.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN Client and VPN router to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_client.com** as the local ID for the VPN Client. 2
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_router.com** as the remote ID for the VPN router. 3

7. Specify the global parameters:

   a. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

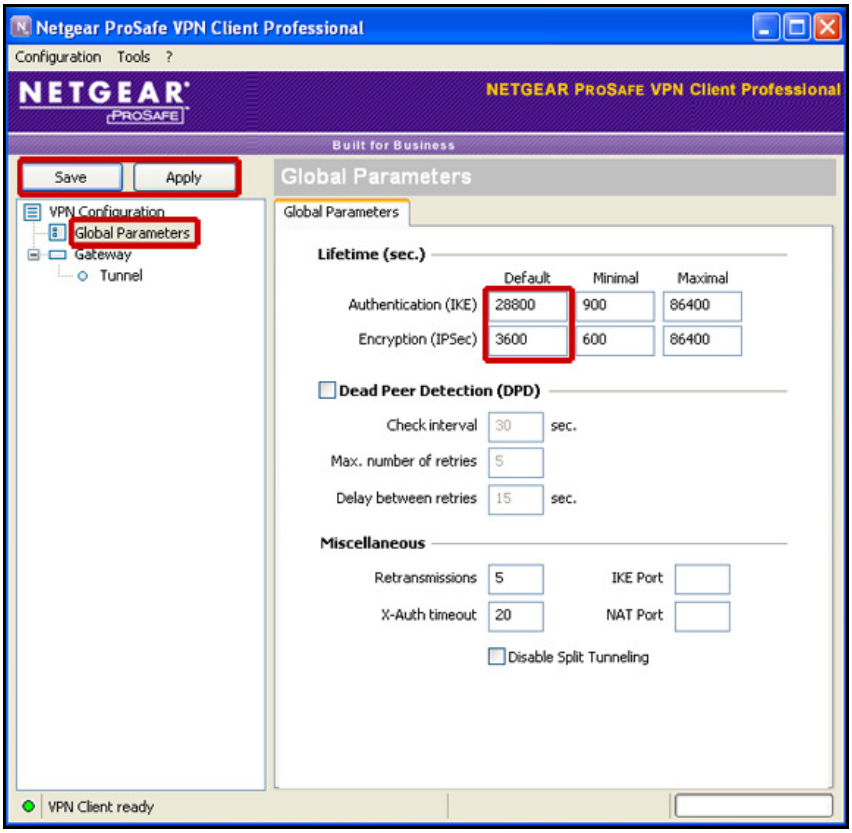


Figure 79.

   b. Specify the default lifetimes in seconds:

   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN router.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN router.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN Client configuration is now complete.

For information about how to connect the VPN Client to the VPN router, see *Establish a VPN connection* on page 114.

Manually Configure the VPN Client

To manually configure a VPN connection between the VPN Client and a router, access the VPN Client's user interface, create authentication settings (phase 1 settings) and an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Authentication Settings (Phase 1 Settings)

➢ **To create new authentication settings:**

1. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration** and select **New Phase 1**.

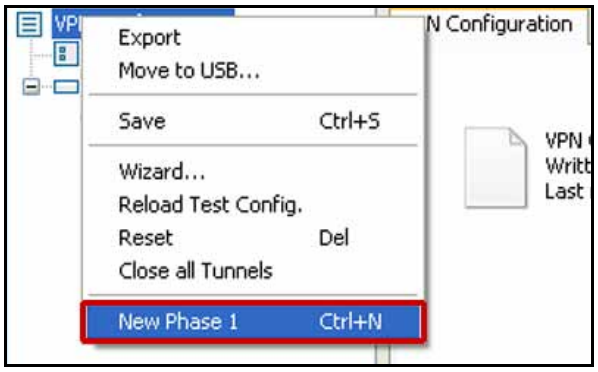


Figure 80.

2. Change the name of the authentication phase name (the default is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **vpn_client**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the authentication phase that is used only for the VPN Client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

   The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

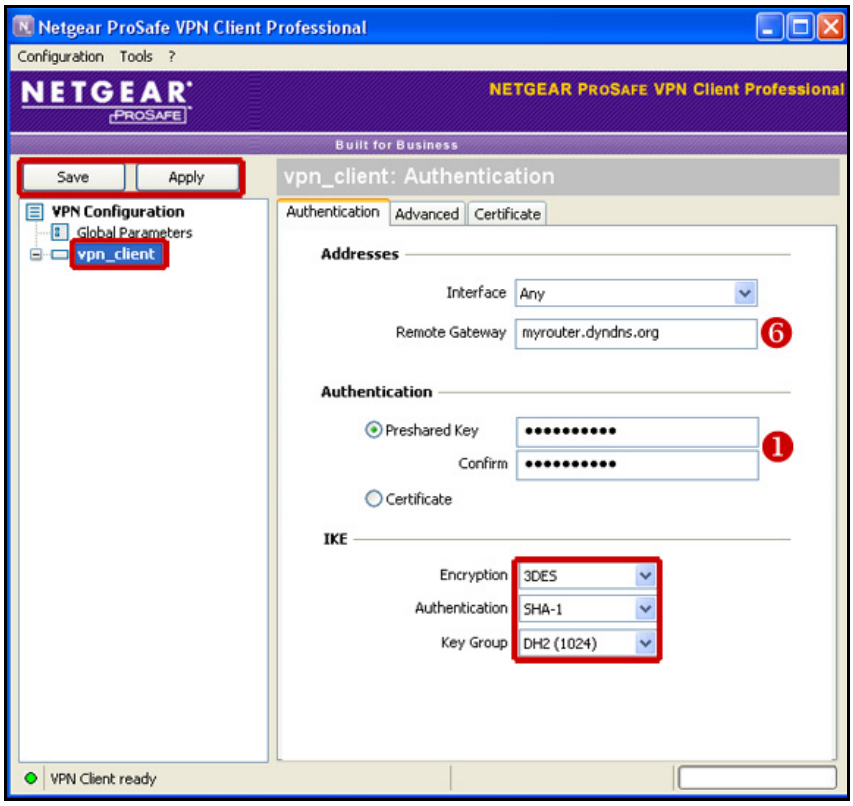


Figure 81.

3. Specify the settings that are explained in the following table.

Table 17. VPN Client authentication settings

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN router. for example, **myrouter.dyndns.org** or **10.200.13.18**. 6	
Preshared Key	Select the **Preshared Key** radio button. Enter **N3tg4ar12**, which is the preshared key that you already specified on the VPN router. 1 Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
5. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays:

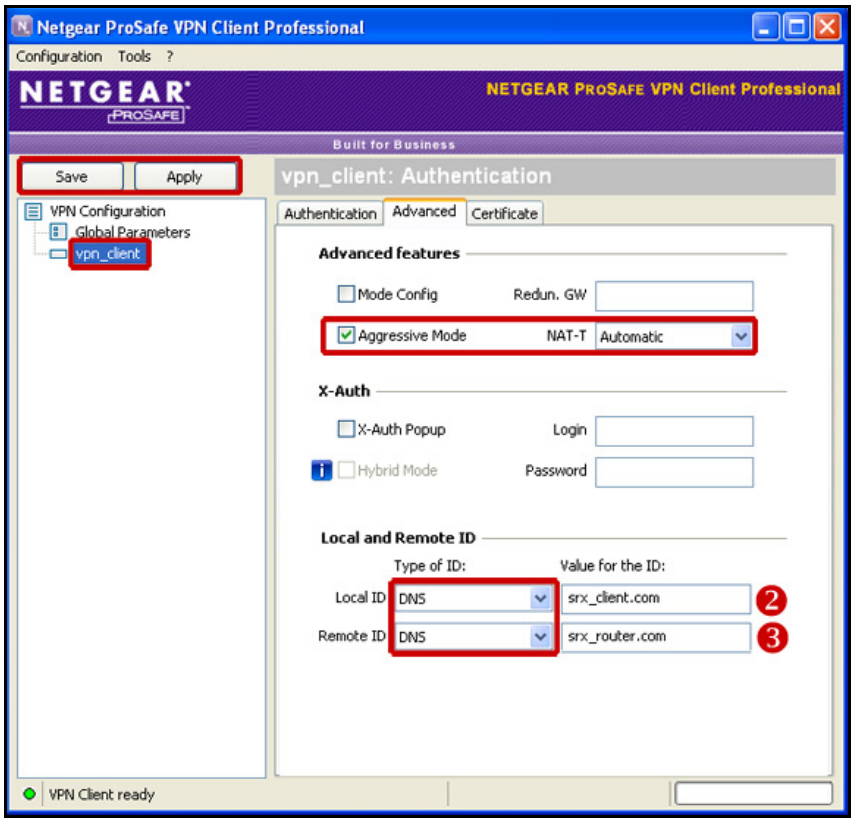


Figure 82.

6. Specify the settings that are explained in the following table.

Table 18. VPN Client advanced authentication settings

Setting	Description
Advanced Features	
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN router.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN Client and VPN router to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_client.com** as the local ID for the VPN Client. ❷
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified **FQDN** in the VPN router configuration. As the value of the ID, enter **srx_router.com** as the remote ID for the VPN router. ❸

7. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the IPSec Configuration (Phase 2 Settings)

> ***Note:*** On NETGEAR routers, the IPSec configuration phase 2 settings) is referred to as the VPN settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name, and then select **New Phase 2**.

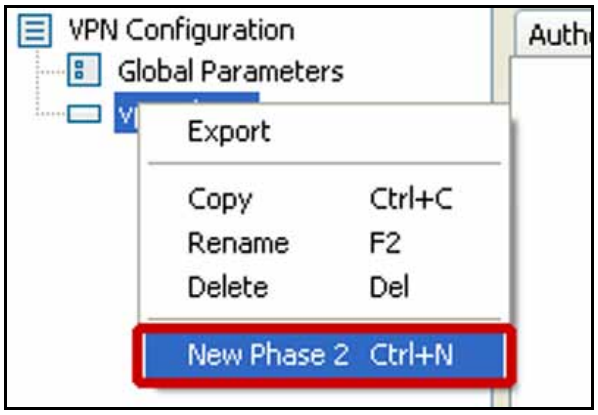


Figure 83.

2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **SRX5308**.
   d. Click anywhere in the tree list pane.

> ***Note:*** *This is the name for the IPSec configuration that is used only for the VPN Client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.

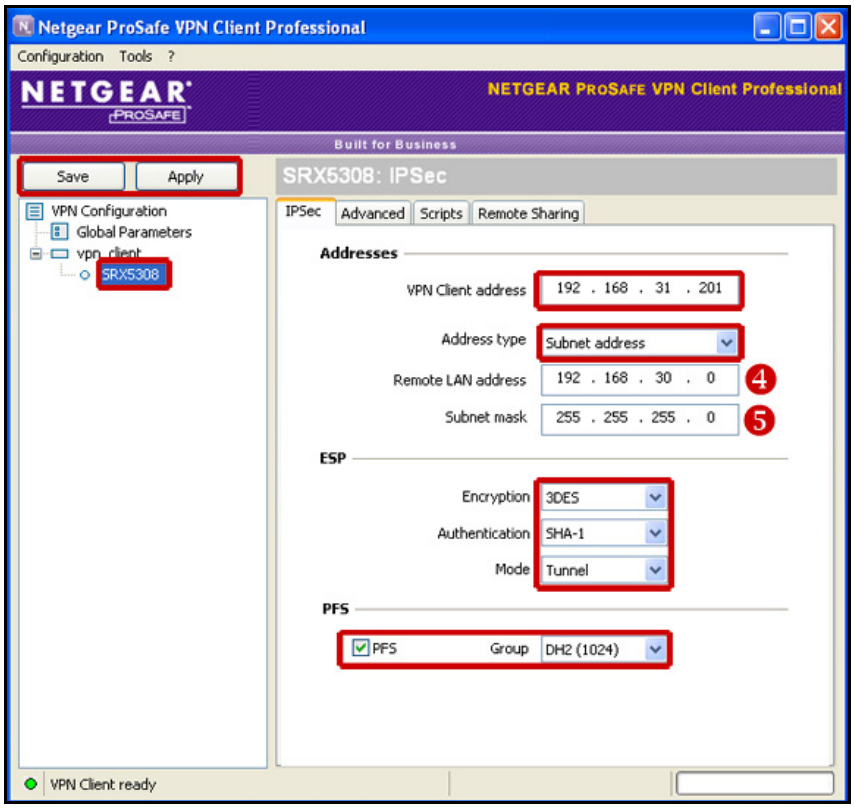


Figure 84.

3. Specify the settings that are explained in the following table.

Table 19. VPN Client IPSec configuration settings

Setting	Description
VPN Client address	Enter **192.168.31.201**. This is the virtual IP address that is used by the VPN Client in the VPN router's LAN; the computer (for which the VPN Client opened a tunnel) appears in the LAN with this IP address. You can also enter another LAN IP address or even **0.0.0.0** as the IP address.
Address Type	Select **Subnet address** from the drop-down list. This selection defines what the VPN Client can communicate with after the VPN tunnel is established.
Remote LAN address	Enter **192.168.30.0** as the remote IP address, or LAN network address, of the gateway that opens the VPN tunnel. 4
Subnet Mask	Enter **255.255.255.0** as the remote subnet mask of the gateway that opens the VPN tunnel. 5

Table 19. VPN Client IPSec configuration settings (continued)

Setting	Description	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On NETGEAR routers, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Global Parameters

➤ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.

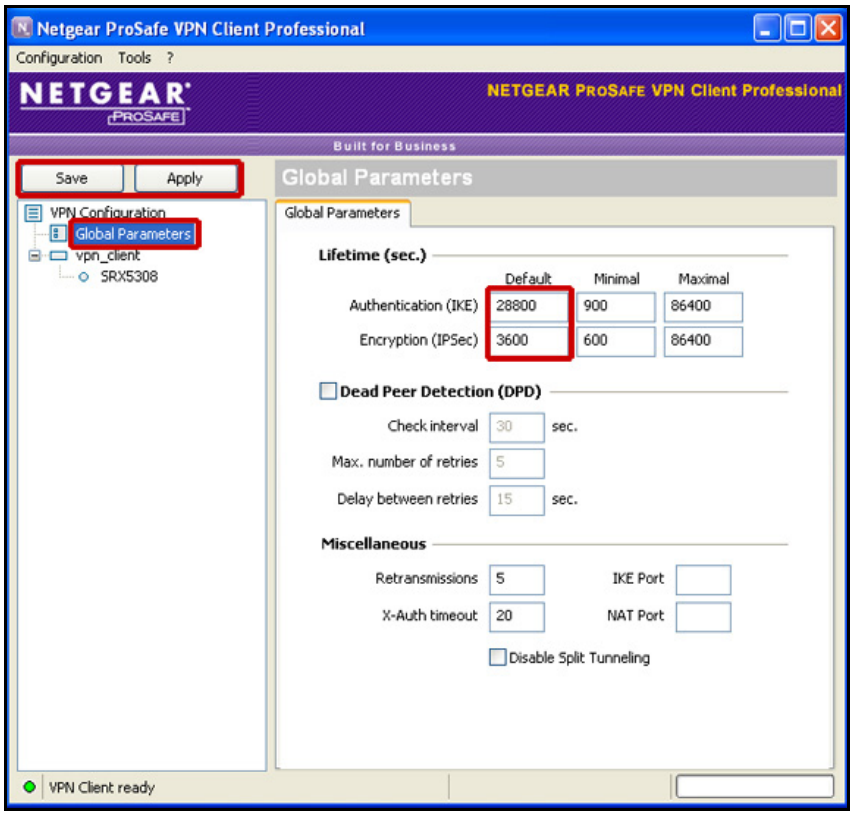


Figure 85.

2. Specify the default lifetimes in seconds:
   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN router.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN router.
3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN Client configuration is now complete.

For information about how to connect the VPN Client to the VPN router, see the next section.

Establish a VPN connection

There are many ways to establish a connection. (The following procedures assume that you changed the authentication phase name to vpn_client and the IPSec configuration to SRX5308. If you did not, the default names are Gateway for the authentication phase name and Tunnel for the IPSec configuration.)

➢ **To establish a connection, use one of the following three methods:**

- **Use the Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:
  - Click the **SRX5308** IPSec configuration name and press **Ctrl + O**.
  - Right-click the **SRX5308** IPSec configuration name and select **Open tunnel**.

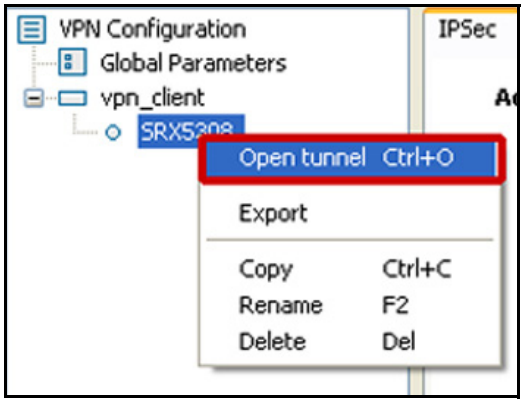


Figure 86.

- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen.

  Perform *one* of the following tasks:
  - Double-click **vpn_client-SRX5308**.
  - Right-click **vpn_client-SRX5308** and click **Open tunnel**.
  - Click **vpn_client-SRX5308** and press **Ctrl + O**.

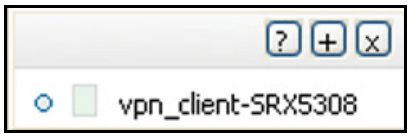


Figure 87.

- **Use the system-tray icon**. Right-click the system tray icon and click **Open 'vpn_client-SRX5308'**.

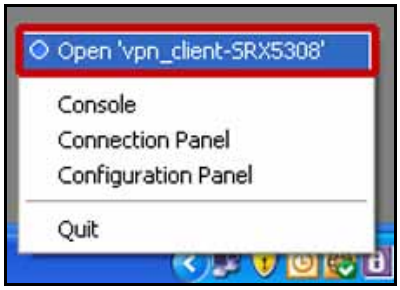


Figure 88.

Note: After the tunnel has been established, the system tray icon changes from purple to green .

VPN Troubleshooting

9

This chapter contains troubleshooting procedures for the VPN Client. This chapter includes the following sections:

- *Overview*
- *Resolving Firewall Interference*
- *Typical Errors*
- *Other Common Problems*
- *View the Logs*

Overview

You can find information about the VPN connection state, VPN traces, and VPN logs on the VPN Console Active screen (see *VPN Console Active Screen* on page 33).

Be careful when configuring an IPSec VPN tunnel. One missing parameter can prevent a VPN connection from being established. Some tools are available to find the source of VPN connection problems. For example, Wireshark is a good and free network analysis software tool (see *http://www.wireshark.org/*) that shows IP or TCP packets that are received on a network card. You can use this tool for packet and traffic analysis, and to follow the protocol exchange between two devices.

Note: For difficulties with software activation, see *Troubleshooting Activation* on page 17.

Note: For difficulties with certificates, see *Certificate Troubleshooting* on page 74.

Resolving Firewall Interference

If you cannot establish a VPN tunnel, your firewall might be interfering. Create firewall rules that allow all traffic to and from the following ports:

- TCP port 500
- UDP port 500
- TCP port 4500
- UDP port 4500

Typical Errors

The following typical errors might occur on the VPN Client:

> ***Note:*** Dates, times, and numbers that can precede the actual messages have been removed from these examples.

"PAYLOAD MALFORMED" Error (Wrong Phase 1 [SA])

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [NOTIFY]
Default exchange_run: exchange_validate failed
Default dropped message from 195.100.205.114 port 500 due to notification type
PAYLOAD_MALFORMED
Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error
```

Explanation: The phase 1 [SA] configuration might be incorrect.

Resolution: Ensure that the encryption algorithms are the same on each side of the VPN tunnel.

"INVALID COOKIE" Error

VPN Console Log:

```
Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
Default dropped message from 195.100.205.114 port 500 due to notification type
INVALID_COOKIE
```

```
Default SEND Informational [NOTIFY] with INVALID_COOKIE error
```

Explanation: One of the endpoints attempts to use an SA that is no longer alive.

Resolution: Reset the VPN connection on each side of the VPN tunnel.

“no keystate” Error

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Explanation: The preshared key or local ID might be incorrect. The logs of the remote endpoint might provide additional information.

Resolution: Ensure that you use the same preshared key on each side of the VPN tunnel and that the local IDs are correctly defined. For the VPN Client, see *Configure Advanced Authentication* on page 47.

”received remote ID other than expected” Error

VPN Console Log:

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
Default ike_phase_1_recv_ID: received remote ID other than expected
```

Explanation: The value of the Remote ID field does not match the value that the remote endpoint is expecting.

Resolution: Ensure that you use the correct value in the Remote ID field on the VPN Client (see *Configure Advanced Authentication* on page 47).

“NO PROPOSAL CHOSEN” Error (Phase 1)

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

Explanation: The phase 1 encryption algorithms might mismatch on the tunnel endpoints.

Resolution: Ensure that the phase 1 IKE encryption algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Configure Authentication* on page 45.

“NO PROPOSAL CHOSEN” Error (Phase 2)

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.1.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
Default RECV Informational [HASH][DEL]
Default Cnx-P1 deleted
```

Explanation: The phase 2 encryption algorithms might mismatch on the tunnel endpoints.

Resolution: Ensure that the phase 2 ESP encryption algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Configure IPSec* on page 52.

“INVALID ID INFORMATION” Error

```
Default sysdep_app_open: Init Connection for : Cnx-Cnx-P2 Cnx-remote-addr
Default sysdep_app_open: IPV4_SUBNET Network 192.168.3.1
Default sysdep_app_open: IPV4_SUBNET Netmask 255.255.255.0
Default (SA Cnx-P1) SEND phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) RECV phase 1 Main Mode [SA][VID]
Default (SA Cnx-P1) SEND phase 1 Main Mode [KEY][NONCE]
Default (SA Cnx-P1) RECV phase 1 Main Mode [KEY][NONCE]
```

```
Default (SA Cnx-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
Default (SA Cnx-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
Default (SA Cnx-Cnx-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
Default RECV Informational [HASH][DEL]
Default Cnx-P1 deleted
```

Explanation: An address might mismatch on the tunnel endpoints, or an SA might no longer be alive.

Resolution: Ensure that both the phase 2 address types and phase 2 address values (see *Configure IPSec* on page 52) match the remote endpoint's address configuration. Ensure that no old SA is still alive on the VPN router.

Other Common Problems

Note: Dates, times, and numbers that can precede the actual messages have been removed from these examples.

There Is No Response to a Phase 1 Request

VPN Console Log:

```
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
```

Explanation: The remote gateway does not answer because some phase 1 settings mismatch on the tunnel endpoints.

Resolution: Ensure that the algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Configure Authentication* on page 45.

Also ensure that the local and remote IDs are correctly specified on each side of the VPN tunnel. For the VPN Client, see *Configure Advanced Authentication* on page 47.

The Console Shows Only “SEND” and “RECV”

VPN Console Log:

```
Default (SA CnxVpn1-P1) SEND phase 1 Aggressive Mode [SA] [KEY_EXCH] [NONCE]
[ID] [VID]
Default (SA CnxVpn1-P1) RECV phase 1 Aggressive Mode
[HASH][SA][KEY_EXCH][NONCE] [ID] [VID]
```

Explanation: The preshared key might mismatch on the tunnel endpoints.

Resolution: Ensure that you use the same preshared key on each side of the VPN tunnel, and there is not a second VPN tunnel to the VPN Client on the VPN router.

There Is No Response to a Phase 2 Requests

VPN Console Log:

```
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
Default (SA CnxVpn1-CnxVpn1-P2) SEND phase 2 Quick Mode [HASH] [SA] [NONCE] [ID]
[ID]
```

Explanation: The phase 2 encryption algorithms or phase 2 addresses might mismatch on the tunnel endpoints.

Resolution: Ensure that the phase 2 ESP encryption algorithms are the same on each side of the VPN tunnel. For the VPN Client, see *Configure IPSec* on page 52.

Ensure that both the phase 2 address types and phase 2 address values (see *Configure IPSec* on page 52) match the remote endpoint’s address configuration.

A Tunnel No Longer Opens

Resolution: Read the logs for each VPN tunnel endpoint. IKE requests might have been dropped by a firewall. The VPN Client needs to be able to use UDP port 500 and ESP port 50.

A VPN Tunnel Is Up but You Cannot Ping the Remote Endpoint

If a VPN tunnel is up but you cannot ping the remote endpoint, check the following:

- Verify that the phase 2 settings are correct, in particular that the VPN Client address and the remote LAN address are correct. Normally the VPN Client address should not belong to the remote LAN subnet.

- When a VPN tunnel is up, packets are sent with the Encapsulating Security Payload (ESP) protocol that could be blocked by a firewall. Verify that all devices between the VPN Client and the VPN router accept the ESP protocol.
- Look at the VPN router logs. Packets might have been dropped by one of its firewall rules.
- Verify that your ISP supports ESP.
- Use a network analysis software tool (such as the free Wireshark tool; *see http://www.wireshark.org/*) to analyze ICMP traffic on the LAN interface of the VPN router and on the LAN interface of the computer to see if encryption functions correctly.
- Verify that the VPN router's LAN default gateway is correctly specified. A target on the remote LAN might receive pings but might not answer because there is no default gateway specified.
- Verify that the computers in the LAN are specified by their IP address and not by their FQDN.
- Use a network analysis software tool (such as the free Wireshark tool; see *http://www.wireshark.org/*) on one of the target computers to verify that the ping arrives inside the LAN.

View the Logs

For information about how to view the VPN logs on the VPN Client, see *VPN Console Active Screen* on page 33. The following figure shows an example of VPN logs on a NETGEAR ProSafe VPN Firewall SRX5308 router.

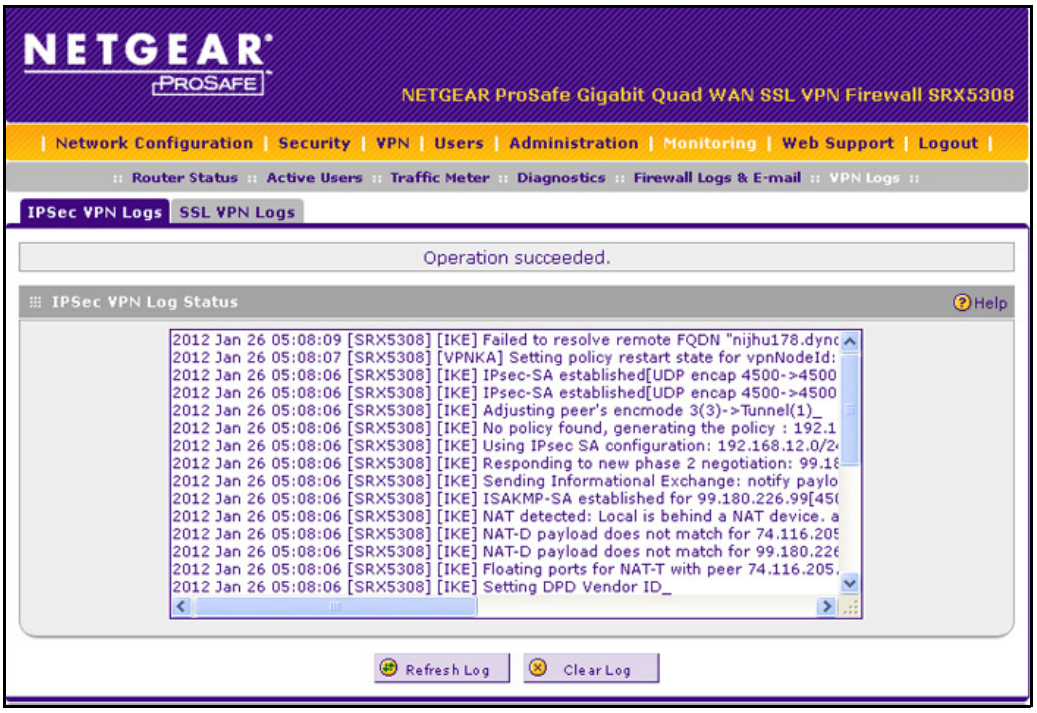


Figure 89.

Following is an example of a VPN log on the VPN router after a VPN Client has successfully established a VPN connection with the VPN router. (This example does note relate to the information that is shown in the previous screen; in addition, the date and times that precede the actual messages have been removed from this example).

```
[SRX5308] [IKE] Remote configuration for identifier "srx_client.com" found_
[SRX5308] [IKE] Received request for new phase 1 negotiation:
10.200.13.18[500]<=>116.66.200.178[885]_
[SRX5308] [IKE] Beginning Aggressive mode._
[SRX5308] [IKE] Received unknown Vendor ID_
[SRX5308] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02__
[SRX5308] [IKE] Received unknown Vendor ID_
[SRX5308] [IKE] For 116.66.200.178[885], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
[SRX5308] [IKE] Floating ports for NAT-T with peer 116.66.200.178[28950]_
[SRX5308] [IKE] NAT-D payload does not match for 10.200.13.18[4500]_
[SRX5308] [IKE] NAT-D payload does not match for 116.66.200.178[28950]_
[SRX5308] [IKE] NAT detected: Local is behind a NAT device. and alsoPeer is
behind a NAT device_
[SRX5308] [IKE] ISAKMP-SA established for
10.200.13.18[4500]-116.66.200.178[28950] with
spi:14e465c525b13972:87ea734ec64e1c97_
[SRX5308] [IKE] Sending Informational Exchange: notify
payload[INITIAL-CONTACT]_
```

```
[SRX5308] [IKE] Responding to new phase 2 negotiation: 10.200.13.18[0]<=
>116.66.200.178[0]_
[SRX5308] [IKE] Using IPsec SA configuration: 192.168.30.0/24<->0.0.0.0/0 from
srx_client.com_
[SRX5308] [IKE] No policy found, generating the policy : 192.168.31.201/32[0]
192.168.30.0/24[0] proto=any dir=in_
[SRX5308] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)_
[SRX5308] [IKE] IPsec-SA established [UDP encap 28950->4500]: ESP/Tunnel
116.66.200.178->10.200.13.18 with spi=8414587(0x80657b)_
```

VPN Client Software Setup Deployment and Command-Line Interface Guide

A

This appendix is an extension of the *VPN Client Software Setup and Deployment* chapter and duplicates some information that is also presented in the chapter. The appendix describes further management and software setup configuration options for the VPN Client and provides examples that illustrate how to manage the software; it includes the following sections:

- *Overview*
- *VPN Client Software Setup Deployment*
- *Customize VPN Client Software for End Users*
- *VPN Configuration Deployment*
- *VPN Automations*
- *Software Setup Command Reference*
- *Command-Line Interface Command Reference*

> ***Note:*** The information in this appendix is typically used by network administrators.

Overview

The following are some of the options that you can integrate in the installation process of the VPN Client:

- The license number for activation
- The email address for activation
- The mode in which the VPN Client starts
- Whether or not the user interface is hidden, and if so, to what degree

The following are some of the options that you can specify to be automatically configured after the VPN Client has been installed:

- If and how the VPN configuration is imported
- If and how a VPN tunnel starts and stops automatically
- If and how the VPN Client starts and quits automatically

You can deploy the VPN Client software setup installation package using several media:

- **Network drive**. Enables users to download and install the VPN Client by simply double-clicking an icon.
- **CD-ROM disk**. Enables users to insert the VPN Client installation CD, and the installation will run automatically (AutoPlay).
- **USB drive**. Enables you to carry the installation package with you, insert the USB drive into a user's computer, and let the installation run automatically.

VPN Client Software Setup Deployment

Silent Installation

The VPN Client software deployment mainly lets the software setup run silently. A silent VPN Client software setup is an installation that is automatically processed without user input through the use of software setup commands. The VPN Client software setup is specifically designed to run silently.

A silent installation uses installation parameters (software setup commands) that are delivered through the CLI.

To improve the transparency of the installation, the VPN Client software setup also lets you add specific CLI commands to customize the software setup installation. For more information, see *Software Setup Command Reference* on page 135.

Create a Silent VPN Client Software Setup

➢ **To create a silent VPN Client software setup:**

1. Download the vpn_client.exe setup file or copy it from the installation CD.
2. Open a command screen, and enter the following software setup commands:

   ```
   [software path][name]_setup.exe /S --lang=[code] --license=[number]
   --start=1 /D=[install path] [CLI commands]
   ```

   in which

   `[software path]` is the path to the setup software file.

   `[name]` is the name of the setup software file

   `[code]` is the language code

   `[number]` is the license number

   `[install path]` is the path to the directory where the setup software file is installed.

   `[CLI commands]` are the optional CLI commands that you can add.

   Note: *Do not include the brackets in the software setup commands.*

The following is an example of the syntax for a software setup:

```
C:\Users\bob\Downloads\NETGEARVPNClientPro_setup.exe /S --lang=1036
--license=123456789 --start=1 /D=c:\Program Files\NETGEAR\NETGEAR VPN
Client Professional
```

Note: The directory that is specified after the **/D** switch needs to specify the path entirely. This switch does not recognize a relative directory. The **/D** switch needs to be the last switch in the command line.

Note: You need to specify a software setup command that requires a parameter without a space between the command and the parameter. Quotation marks are required if the parameter contains spaces, for example, “C:\Temporary Downloads\Program Files”. However, if there are spaces in the installation path **[install path]**, quotation marks are not required.

Deploy a VPN Client Software Setup from a CD-ROM

➢ **To deploy a VPN Client software setup from a CD-ROM:**

1. Create a silent VPN Client software setup.
2. Create an autorun file by creating a text file and saving it as **autorun.inf**. Upon CD-ROM insertion, this autorun file is used by the operating system to automatically run the VPN Client software installation.
3. Place the following content in the autorun.inf file:

   ```
   [autorun]
   OPEN=[cdpath\]VPN_Client.exe /S /D=[install path] [optional CLI commands]
   ICON=[cdpath\]VPN_Client.exe
   ```

   in which

   [install path] is the path to the directory where the setup software file is installed.

   [CLI commands] are the optional CLI commands that you can add.

   Note: *Do not include the brackets in the software setup commands.*

4. Copy the content of the setup directory and the autorun.inf file to the root directory of the CD-ROM.

The following is an example of the syntax for a software setup:

```
[autorun]
OPEN=VPN_Client.exe /S --start=1 --lang=1036 --license=123456789 /D=
c:\Program Files\NETGEAR\NETGEAR VPN Client Professional
ICON=VPN_Client.exe
```

Run a VPN Client Software Setup from a Shortcut (Double-Click an Icon)

➢ **To run a VPN Client software setup from a shortcut:**

1. Create a silent VPN Client software setup.
2. Right-click the **setup.exe** file in the setup directory, and from the popup menu, select **Create Shortcut**. A shortcut to the setup.exe file in the setup directory is created.
3. Right-click the new shortcut, and from the popup menu select **Properties**. In the Target field, add the following software setup commands to the command line:

   `/S --start=1 --lang=[code] --license=[number] /D=[install path]`

   in which

   in which

   `[install path]` is the path to the directory where the setup software file is installed.

   Note: *Do not include the brackets in the software setup commands.*

   The following is an example of the syntax for a software setup:

   ```
   C:\Users\bob\Downloads\NETGEARVPNClientPro_Setup.exe /S --lang=1036
   --license=123456789 --start=1 /D=C:\Program Files\NETGEAR\NETGEAR VPN
   Client Professional
   ```

   IMPORTANT:

   Place a space character following each command as is shown in the example.

4. Move the shortcut to a location where it can be easily clicked by the user (for example, on the desktop).

Deploy a VPN Client Software Setup Using a Batch Script

➢ **To deploy a VPN Client software setup using a batch script:**

1. Create a silent VPN Client software setup.
2. Create a text file with a .bat extension, for example, VPN Client Setup.bat.

3. Edit this file (that is, right-click the file and select **modify** with the commands that you want to be processed, for example:

```
cd .\setup
setup.exe /S –-lang=1036
cd ..
copy myvpnconfig.tgb C:\Program Files\NETGEAR\NETGEAR VPN Client
Professional
cd C:\Program Files\VPN
vpnconf.exe /importance:myvpnconfig.tgb
```

In this example, the setup directory is called setup and is located under the directory that contains the batch file; a VPN configuration is imported at the end of the installation.

4. Deploy this file from a server or on a USB stick together with the setup directory to the users.

Deploy a VPN Client Software Setup from a Network Drive

➢ **To deploy a VPN Client software setup from a network drive:**

1. Create a silent VPN Client software setup on a network drive.
2. Right-click the **setup.exe** file in the setup directory, and from the popup menu, select **Create Shortcut**. A shortcut to the setup.exe file in the setup directory is created.
3. Right-click the new shortcut, and from the popup menu, select **Properties**. In the Target field, add the following software setup commands to the command line:

   `/S --start=1 --lang=[code] --license=[number] /D=[install path]`

   in which

   `[code]` is the language code

   `[number]` is the license number

   `[install path]` is the path to the directory where the setup software file is installed.

   Note: *Do not include the brackets in the software setup commands.*

   The following is an example of the syntax for a software setup:

```
F:\NETGEARVPNClientPro_Setup.exe /S --start=1 --lang=1036 --license=
123456789 /D=C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

IMPORTANT:

Place a space character following each command as is shown in the example.

4. Move the shortcut to a location where it can be easily clicked by the user (for example, on the desktop).

Deploy a VPN Client Software Update

➢ **To deploy a VPN Client software update:**

Launch the silent installation only for the new software release.

The entire uninstallation of the old software release and installation of the new software release is silent; no user action is required.

Customize VPN Client Software for End Users

End users can access the VPN Client in three ways:

- By opening the Configuration Panel screen. This screen is typically used by network administrators and can be hidden or protected by a password.
- By opening the Connection Panel screen. This screen lets the end user open and close tunnels. You can hide this screen.
- By right-clicking the system tray icon and opening the system tray menu. With the exception of the tunnels (these are always shown), you can hide most menu items of the system tray menu.

These access methods enable the network administrator to hide the configuration options from the end user to prevent misuse of the VPN configuration, and to present the end user with simple access to the VPN Client and VPN tunnels.

Note: The VPN configuration is signed and encrypted. Manual editing of the file disables the VPN configuration.

The VPN Client software setup options that enable you to limit access to the VPN Client's configuration options are described in the following sections.

Limit Usage of the VPN Client to the Connection Panel

➢ **To limit usage of the VPN Client to the Connection Panel:**

1. Open the VPN Client's user interface.
2. On the Configuration Panel screen, from the main menu select **Tools > Options**. The Options screen displays with the General pane selected by default.
3. In the Password and Confirm fields, enter and then confirm a password.
4. As an option, you can limit the number of items that display in the system tray menu.
5. Press **Ctrl + Enter** to switch to the Connection Panel screen.
6. As an option, close the Connection Panel screen.

Now, only the Connection Panel screen is displayed when you open the software (that is, when you click the system tray icon). If an end user wants to open the Configuration Panel screen by pressing **Ctrl + Enter** or by clicking **+** in the Connection Panel screen, the password is automatically requested.

For more information, see *View Pane: Access Control and Hidden Interface* on page 27.

Specify Display of the Connection Panel Screen in a VPN Client Software Setup

- **To specify display of the Connection Panel screen in a VPN Client software setup:**

  Add the **`--guidefs=user`** software setup command to the command line.

  The following is an example of the syntax for a software setup:

  ```
  NETGEARVPNClientPro_Setup.exe /S --guidefs=user /D=C:\Program
  Files\NETGEAR\NETGEAR VPN Client Professional
  ```

  After you have installed the VPN Client and rebooted the computer, the VPN Client starts up and displays the Connection Panel screen.

Limit Usage to the Connection Panel Screen in a VPN Client Software Setup

- **To limit usage to the Connection Panel screen in a VPN Client software setup and protect access to the Configuration Panel screen with a password:**

  Add the **`--guidefs=user --password=mypassword`** software setup commands to the command line.

  `mypassword` is the specified password.

  The following is an example of the syntax for a software setup:

  ```
  NETGEARVPNClientPro_Setup.exe /S --guidefs=user --password=group2 /D=
  C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
  ```

  After you have installed the VPN Client and rebooted the computer, the VPN Client starts up and displays the Connection Panel screen, and access to the Configuration Panel screen is protected by a password.

Limit Usage of the VPN Client to the System Tray Icon Menu in a VPN Client Software Setup

➢ **To limit usage of the VPN Client to the system tray icon menu in a VPN Client software setup and protect access to both the Connection Panel screen and Configuration Panel screen with a password:**

Add the **`--guidefs=hidden --password=mypassword`** software setup commands to the command line.

`mypassword` is the specified password.

The following is an example of the syntax for a software setup:

```
NETGEARVPNClientPro_Setup.exe /S --guidefs=user --password=group2 /D=
C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
```

After you have installed the VPN Client and rebooted the computer, the VPN Client starts up with access to the system tray menu only, and access to both the Connection Panel screen and Configuration Panel screen is protected by a password. You can open and close tunnels from the system tray menu.

VPN Configuration Deployment

The VPN Client software setup lets you embed a preconfigured VPN configuration that is automatically used by the VPN Client during the installation process.

Embed a VPN Configuration in the VPN Client Software Setup

➢ **To embed a VPN configuration in the VPN Client software setup:**

1. Create a VPN configuration. You can do this on any computer on which the VPN Client is installed.
2. Export the VPN configuration (by selecting **Configuration > Export** from the main menu on the Configuration Panel screen), and rename your configuration, for example, to conf.tgb.

> ***Note:*** Do not protect the exported VPN configuration with a password.

3. Add the VPN configuration (that is, the conf.tgb file) to the directory in which you intend to place the software setup file on the target computer. If you intend to use the software setup files on a USB drive, copy the VPN configuration onto the USB drive together with the software setup file.
4. Deploy the package to the user and execute the setup. The VPN configuration (that is, the conf.tgb file) is automatically imported during the software setup process.

Export and Deploy a New VPN Configuration

➢ **To create a VPN Client software setup with an embedded VPN configuration:**

1. Create a VPN configuration. You can do this on any computer on which the VPN Client is installed.
2. Export the VPN configuration (by selecting **Configuration > Export** from the main menu on the Configuration Panel screen), and rename your configuration, for example, to conf.tgb. You *can* protect this exported VPN configuration with a password.
3. Forward the VPN configuration to the end user, either by email or through file sharing.

   When the end user opens the VPN configuration (for example, the end user opens the email attachment), the VPN configuration is automatically imported and applied by the VPN Client. If you have specified a password, it is automatically requested and must be entered by the end user before the VPN configuration is processed.

VPN Automations

Create a Batch or Script That Automatically Opens or Closes a Tunnel

You can open or close a VPN tunnel through a CLI command, even when the VPN Client is running.

➢ **To open a VPN tunnel, enter the following CLI command:**

[path]\vpnconf.exe /open:[NamePhase1-NamePhase2]

in which

`[path]` is the VPN Client installation directory.

`[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

Note: *Do not include the brackets in the software setup commands.*

If the specified tunnel is already open, the CLI command has no effect.

➢ **To close a VPN tunnel, enter the following CLI command:**

[path]\vpnconf.exe /close:[NamePhase1-NamePhase2]

in which

`[path]` is the VPN Client installation directory.

`[NamePhase1-NamePhase2]` are the phase 1 and phase 2 names in the VPN configuration file.

Note: *Do not include the brackets in the software setup commands.*

If the specified tunnel is already closed, the CLI command has no effect.

Note: The **open** and **close** commands are mutually exclusive.

Note: When you enter the **open** or **close** command, the user interface opens. This restriction will be removed in a future software release.

Automatically Open a Web Page When a VPN Tunnel Opens

➢ **To automatically open a Web page when a VPN tunnel opens:**

1. Create a VPN configuration.
2. In the IPSec pane of the Configuration Panel screen, click the **Scripts** tab. The Scripts pane displays (see *Figure 43* on page 58).
3. In the Launch this script when this tunnel opens field, enter the URL of the Web page that you want to be opened, for example, http://kb.netgear.com/app/products/list/p3/315.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

When the tunnel for which the script is defined opens, the Web page is opened.

Open a Tunnel with a Double-Click on a Desktop Icon

➢ **To open a tunnel with a double-click on a desktop icon:**

1. Create a VPN configuration.
2. In the Advanced authentication pane of the Configuration Panel screen (see *Figure 41* on page 56), select the **Automatically open this tunnel when the VPN Client starts after login** check box.
3. Export the VPN configuration to a file by selecting **Configuration > Export** from the main menu on the Configuration Panel screen.
4. Place a shortcut of the VPN configuration file on the desktop.

When you double-click the desktop icon, the VPN Client opens with the specified VPN configuration, and the tunnel is then automatically opened.

Software Setup Command Reference

The following table lists the software setup switches and commands that are available to customize the VPN Client software setup.

Note: The software setup commands that are described in this section need to be used together with the **/S** switch (silent mode uninstallation followed by installation, case-sensitive).

Note: When you specify a software setup command that requires a parameter, do not place a space between the command and the parameter. Quotation marks are required if the parameter contains spaces. However, if there are spaces in the installation path **[install path]**, quotation marks are not required.

Table 20. Software setup switches and commands

Switch or Command	Description
/D=[install path]	**[install path]** is the path where the VPN Client is installed. **Note:** **D** needs to be preceded by only one slash and is case-sensitive. Quotation marks are not allowed, even if there is a space in the path. **Note:** **/D** needs to be placed at the end of the command line, as the last option, and you need to use it with the **/S** option (silent mode). **Example**: NETGEARVPNClientPro_Setup.exe /S --guidefs=user /D= C:\Program Files\NETGEAR\NETGEAR VPN Client Professional
/S	Enables a silent uninstallation of an already installed version followed by a silent installation of a specified version (no dialogs are displayed during the uninstallation and installation). **Note:** **S** needs to be preceded by only one slash and is case-sensitive. **Note:** If there is no version installed, the uninstallation is ignored. **Example**: NETGEARVPNClientPro_Setup.exe /S

Table 20. Software setup switches and commands (continued)

Switch or Command	Description
--activmail=[activation_email]	Lets you configure and automatically enter the email that is used for activation confirmation. During the activation process, the field that is used to enter the email is disabled. **`[activation_email]`** is the email that is required for activation. **Note:** **`activmail`** needs to be preceded by two hyphens (**`--`**). **Example**: NETGEARVPNClientPro_Setup.exe /S --activmail= salesgroup@company.com
--autoactiv=1	Activates the VPN Client automatically when the network is available during startup or when there is a request to open a tunnel. This option requires that the license number and activation email have already been entered in a previous installation. **Note:** **`--autoactiv=1`** needs to be the last command in the command line. **Note:** **`autoactiv=1`** needs to be preceded by two hyphens (**`--`**). **Example**: NETGEARVPNClientPro_Setup.exe /S --autoactiv=1
--guidefs=[full|user|hidden]	Configures the user interface appearance when the VPN Client starts. • **full**. The Configuration Panel screen is displayed. This is the default setting. • **user**. The Connection Panel screen is displayed. • **hidden**. Neither the Configuration Panel screen nor the Connection Panel screen is displayed. Only the system tray menu can be opened. Tunnels can be opened from the system tray menu. **Note:** **`guidefs`** needs to be preceded by two hyphens (**`--`**). **Example**: NETGEARVPNClientPro_Setup.exe /S --guidefs=hidden

Table 20. Software setup switches and commands (continued)

<table>
<tr><th>Switch or Command</th><th colspan="3">Description</th></tr>
<tr><td>--lang=[language code]</td><td colspan="3">Specifies the language for the software setup and for the VPN Client.
<code>[language code]</code> is the code for the language. The codes are shown in the following rows in this table.

Note: <code>lang</code> needs to be preceded by two hyphens (<code>--</code>).

Example:
NETGEARVPNClientPro_Setup.exe /S --lang=1040</td></tr>
<tr><td></td><td>ISO 639-2 Code</td><td>Language Code</td><td>English Name</td></tr>
<tr><td></td><td>AR</td><td>1025</td><td>Arabic</td></tr>
<tr><td></td><td>CZ</td><td>1029</td><td>Czech</td></tr>
<tr><td></td><td>DK</td><td>1030</td><td>Danish</td></tr>
<tr><td></td><td>DE</td><td>1031</td><td>German</td></tr>
<tr><td></td><td>EL</td><td>1032</td><td>Greek</td></tr>
<tr><td></td><td>EN</td><td>1033 (default)</td><td>English</td></tr>
<tr><td></td><td>ES</td><td>1034</td><td>Spanish</td></tr>
<tr><td></td><td>FI</td><td>1035</td><td>Finnish</td></tr>
<tr><td></td><td>FR</td><td>1036</td><td>French</td></tr>
<tr><td></td><td>HU</td><td>1038</td><td>Hungarian</td></tr>
<tr><td></td><td>IT</td><td>1040</td><td>Italian</td></tr>
<tr><td></td><td>JA</td><td>1041</td><td>Japanese</td></tr>
<tr><td></td><td>NL</td><td>1043</td><td>Dutch</td></tr>
<tr><td></td><td>NO</td><td>1044</td><td>Norwegian</td></tr>
<tr><td></td><td>PL</td><td>1045</td><td>Polish</td></tr>
<tr><td></td><td>RU</td><td>1049</td><td>Russian</td></tr>
<tr><td></td><td>TH</td><td>1054</td><td>Thai</td></tr>
<tr><td></td><td>TR</td><td>1055</td><td>Turkish</td></tr>
<tr><td></td><td>SL</td><td>1060</td><td>Slovenian</td></tr>
<tr><td></td><td>HI</td><td>1081</td><td>Hindi</td></tr>
<tr><td></td><td>ZH</td><td>2052</td><td>Chinese simplified</td></tr>
<tr><td></td><td>PT</td><td>2070</td><td>Portuguese</td></tr>
<tr><td></td><td>SR</td><td>2074</td><td>Serbian</td></tr>
</table>

Table 20. Software setup switches and commands (continued)

Switch or Command	Description
--license=[number]	Lets you configure and automatically enter the license number that is used for activation. **[number]** is the license number that consists of 20 or 24 hexadecimal characters. **Note:** **license** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --license= 1234567890ABCDEF12345678
--menuitem=[0...31]	Specifies the items of the system tray menu that are visible. The value is a bit field: • **1**. Quit menu item displays. • **2**. Connection Panel menu item displays. • **3**. Quit and Connection Panel menu items display. • **4**. Console menu item displays. • **5**. Quit and Console menu items display. • **16**. Configuration Panel menu item displays. • **31**. All menu items display. This is the default setting. **Note:** Tunnels are always shown in the system tray menu and can always be opened and closed from the system tray menu. **Note:** By default, **--guidefs=hidden** sets the system tray menu item list to Quit and Console (that is, the Connection Panel menu items are not visible). However, **--menuitem** overrides **--guidefs**. That means that when you enter **--guidefs= hidden --menuitem=1**, the system tray menu shows the Quit menu item only. **Note:** **menuitem** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --menuitem=3
--noactiv=1	Prevents the Trial screen from displaying when the VPN Client starts until the trial period ends. A user other than the network administrator does not know about the trial period, and the VPN Client is disabled at the end of the trial period. If a user attempts to launch the VPN Client after the end of trial period, the VPN Client starts and opens the Trial screen but the Evaluate button is disabled. **Note:** **noactiv=1** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --noactiv=1

Table 20. Software setup switches and commands (continued)

Switch or Command	Description
--password=[password]	Protects the user interface or a protected screen of the user interface. **[password]** is the password that you need to enter to gain access under the following circumstances. • When you click or double-click the VPN system tray icon. • When you want to switch from the Connection Panel screen to the Configuration Panel screen. **Note:** **password** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --password=adm253q
--**reboot=1**	Automatically reboot the computer after a silent installation of the VPN Client. **Example**: NETGEARVPNClientPro_Setup.exe /S --reboot=1
--start=[1|2]	Configures the start mode for the VPN Client. These are the options: • **1**. The VPN Client starts after Windows login. This is the default setting. • **2**. The VPN Client needs to be started manually. **Note:** **start** needs to be preceded by two hyphens (**--**). **Example**: NETGEARVPNClientPro_Setup.exe /S --start=2

Command-Line Interface Command Reference

You can use command-line interface (CLI) commands to customize the VPN Client software setup. Use CLI commands in batch files, in scripts, or in software setup autorun.inf files.

The following is the standard syntax for CLI commands:

[install_directory]\vpnconf.exe **[/option[:value]]**

in which

[install_directory] is the installation directory of the VPN Client software files.

[/option[:value]] are the CLI command and argument. If the argument contains space characters, place the argument between double quotes.

Note: *Do not include the brackets in the CLI commands.*

The following table lists the CLI commands that are available to customize the VPN Client software setup.

Table 21. CLI commands

Command	Description
/add:[ConfigFileName]	Imports a new VPN configuration into an existing VPN configuration and merges both into a single VPN configuration, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. **`[ConfigFileName]`** is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** This command can replace the **`/importonce:`** command. **Example**: vpnconf.exe /add:"c:\my documents\myvpnconf.tgb"
/close:[NamePhase1-NamePhase2]	Closes a specified VPN tunnel. **`[NamePhase1-NamePhase2]`** are the phase 1 and phase 2 names in the VPN configuration file. **Example**: vpnconf.exe /close:"Home gateway-cnx1" **Note:** In the example, the **`Home gateway-cnx1`** VPN configuration is placed between double quotes because there is a space character in the name.
/export:[ConfigFileName]	Exports the current VPN configuration (including certificates) to the specified file and starts the VPN Client if it is not already running. If the VPN Client is running, the VPN configuration is exported while the VPN Client remains running. **`[ConfigFileName]`** is the name of the file to which the VPN configuration is exported. Enclose this name in double quotes if it contains space characters. This command requires you to also specify a password with the **`/pwd:`** command. **Example**: vpnconf.exe /export:"c:\my documents\myvpnconf.tgb"
/exportonce:[ConfigFileName]	Exports the current VPN configuration (including certificates) to the specified file when the VPN Client is not running and does not start the VPN Client. If the VPN Client is running, the VPN configuration is exported while the VPN Client remains running. **`[ConfigFileName]`** is the name of the file to which the VPN configuration is exported. Enclose this name in double quotes if it contains space characters. This command requires you to also specify a password with the **`/pwd:`** command. **Example**: vpnconf.exe /exportonce:"c:\my documents\myvpnconf.tgb"

Table 21. CLI commands (continued)

Command	Description
/import:[ConfigFileName]	Enables the VPN Client to import a VPN configuration. If the VPN Client is not running, the VPN configuration is imported and the VPN Client is automatically started. If the VPN Client is running, the VPN configuration is imported while the VPN Client remains running. **`[ConfigFileName]`** is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** To prevent the end user from being asked if the new VPN configuration should be added to or replace the existing VPN configuration, enter the **`/add:`** or **`/replace:`** command instead of the **`/import:`** command. **Example**: vpnconf.exe /import:"c:\my documents\myvpnconf.tgb"
/importonce:[ConfigFileName]	Imports a VPN configuration file when the VPN Client is *not* running and does not start the VPN Client. If the VPN Client is running, the VPN configuration is imported while the VPN Client remains running. This command is useful in installation scripts: it allows you to run a silent installation and to automatically import a VPN configuration file without starting the VPN Client. **`[ConfigFileName]`** is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** To prevent the end user from being asked if the new VPN configuration should be added to or replace the existing VPN configuration, enter the **`/add:`** or **`/replace:`** command instead of the **`/importonce:`** command. **Example**: vpnconf.exe /importonce:"c:\my documents\myvpnconf.tgb"
/open:[NamePhase1-NamePhase2]	Opens a specified VPN tunnel. **`[NamePhase1-NamePhase2]`** are the phase 1 and phase 2 names in the VPN configuration file. **Example**: vpnconf.exe /open:Corporate-gateway1

Table 21. CLI commands (continued)

Command	Description
/pwd:[Password]	Enables you to set a password for import and export operations. **[Password]** is the password that you need to enter to enable the command with which the **/pwd:** command is combined. The **/exportonce:** and **/exportonce:** commands require you to set a password. A password is optional for the **/import:**, **/importonce:**, **/add:**, and **/replace:** commands. **Note:** You need to place the **/pwd:** command *after* the other command that you combine the **/pwd:** command with. **Example**: vpnconf.exe /import:"c:\my documents\myvpnconf.tgb" /pwd=mypwd
/replace:[ConfigFileName]	Imports a new VPN configuration into an existing VPN configuration and replaces the old configuration with the new one, whether or not the VPN Client is running. This command does not start the VPN Client if it is not running. **[ConfigFileName]** is the file name of the VPN configuration that is imported. Enclose this name in double quotes if it contains space characters. **Note:** This command can replace the **/importonce:** command. **Example**: vpnconf.exe /replace:"c:\my documents\myvpnconf.tgb"
/stop:	Closes all active tunnels and closes the VPN Client. Use this command, for example, in a script that starts the VPN Client after establishing a dial-up connection and closes it just before disconnecting the dial-up connection. **Example**: vpnconf.exe /stop

Generating Certificates With Microsoft Certificates Services and OpenSSL

B

This appendix is an extension *Certificate Management* on page 66. This appendix includes the following sections:

- *Microsoft Certificates Services*
- *OpenSSL*

> ***Note:*** The information in this chapter is typically used by network administrators.

> ***Note:*** For information about how to import and display certificates, see *Certificate Management* on page 66.

Microsoft Certificates Services

This section describes how to generate a user certificate, sign a certificate signing request (CSR), and export a certificate using Microsoft certificates services.

Install Microsoft Certificate Services

Microsoft certificate services comes as a part of the Windows NT, Windows 2000, and WIndows 2003 server option pack and requires Microsoft Internet Information Server (IIS) and Microsoft Internet Explorer (IE).

The enrollment Web pages that are provided by the certificate services let you connect to the services with a Web browser and perform common tasks such as requesting the certificate authority (CA) and processing a CSR file or smart card enrollment file. The Web pages are located at http://ServerName/CertSrv, in which ServerName is the name of the CA.

The following Microsoft Web pages provide information about certificate services:

- Windows 2000 server:
  http://technet.microsoft.com/en-us/library/cc961642.aspx
- Windows 2003 server:
  http://technet.microsoft.com/en-us/library/cc780742(WS.10).aspx
- Windows 2008 server (Active Directory certificate services):
  http://technet.microsoft.com/en-us/library/cc770357(WS.10).aspx

➢ **To install the Internet Information Server (IIS 6.0):**

1. In Windows, select **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components** (in the left column of the Add or Remove Programs screen).
2. Select **Application Server**, and click **Details**.
3. Select **Internet Information Services (IIS)**, and click **Details**.
4. Select the **World Wide Web Service** check box, and click **OK**.
5. On the Application Server screen, click **OK**.
6. On the Windows Components Wizard screen, click **Next**.
7. On the Completing the Windows Components Wizard screen, click **Finish**.

➢ **To install the Microsoft Certificate Server with a standalone root CA on a Windows 2003 server:**

1. In Windows, select **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components** (in the left column of the Add or Remove Programs screen).
2. Select **Certificate Services**, and click **Details**.
3. Select both the **Certificate Services CA** and **Certificate Services Web Enrollment Support** check boxes, and click **OK**.
4. On the Windows Components Wizard screen, click **Next**.
5. Configure the CA type by selecting the **Stand-alone root CA** radio button and the **Use custom settings to generate the key pair and CA certificate** check box as shown in the following figure, and then click **Next**.

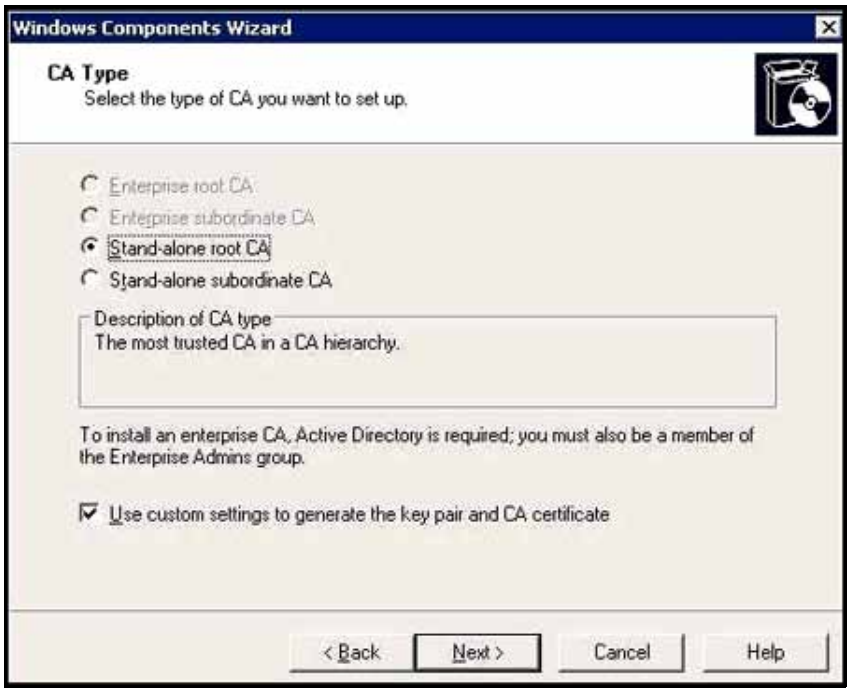


Figure 90.

6. Configure the public and private key pair by selecting **Microsoft Strong Cryptographic Provider** from the CSP drop-down list, **SHA-1** from the Hash algorithm drop-down list, and **1024** from the Key length drop-down list as shown in the following figure, and then click **Next**.

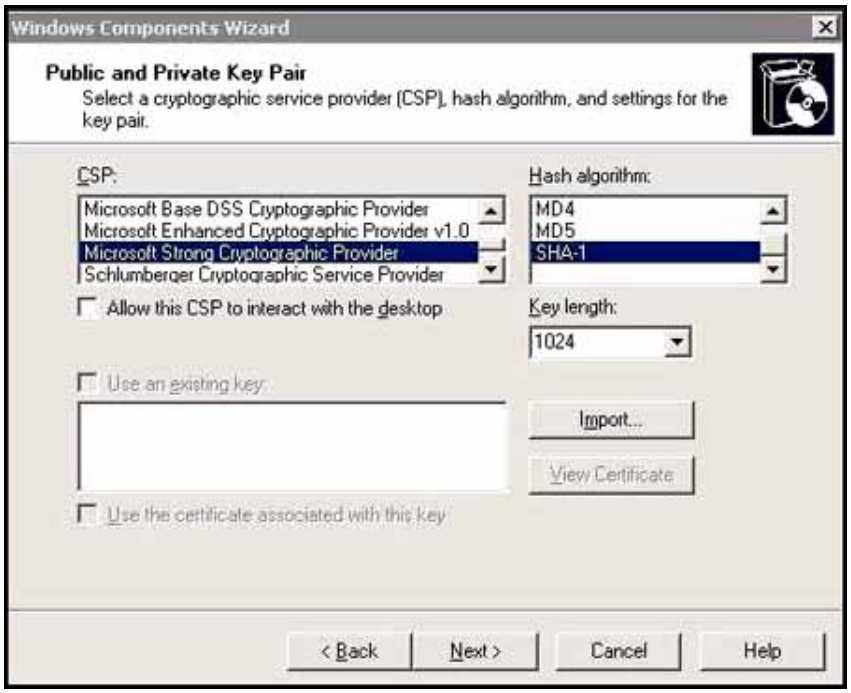


Figure 91.

7. Configure the CA identifying information by entering a common name (**TgbCA** in the example) and distinguished name suffix (**DC=TheGreenBow,DC-fr** in the example) and by selecting a validity period (**10 Years** in the example) as shown in the following figure, and then click **Next**.

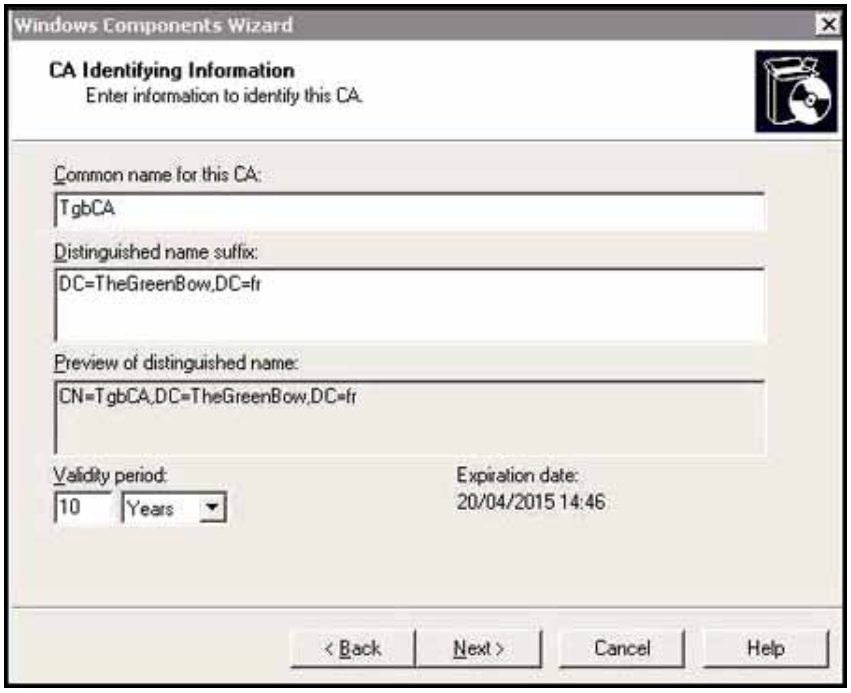


Figure 92.

8. On the Certificate Database Settings screen, use the default locations for the Certificate Database and Certificate Database Log. You do not need to specify a shared folder to store configuration information because this information is stored in the active directory. Click **Next**.
9. On the Microsoft Certificate Services warning screen, click **Yes** to confirm that Internet information services can be stopped temporarily.
10. On the Microsoft Certificate Services warning screen, click **Yes** to confirm that Active Server Pages (ASPs) must be enabled in Internet Information Services (IIS) if you want to use the certificate services Web enrollment site.
11. On the Completing the Windows Components Wizard screen, Click **Finish**.
12. Close the Add or Remove Programs screen.

Generate a User Certificate with Microsoft Certificate Services

This section describes how to generate a user certificate for the VPN Client but also can be applied to any other VPN IPSec endpoint such as a VPN router.

➢ **To generate and install a user certificate:**

1. Connect to your certificate server (http://ServerName/CertSrv in which ServerName is the name of the CA server).
2. On the Welcome screen, select **Request a Certificate**.
3. On the Request a Certificate screen, select **Advanced Certificate Request**.
4. On the Advanced Certificate Request screen, select **Create and submit a request to this CA**.
5. Fill in the fields of the Advanced Certificate Request screen, and select the **Mark keys as exportable** check box in the Key Options section because the VPN Client needs the certificate's private key to establish a tunnel. The following figure shows examples.

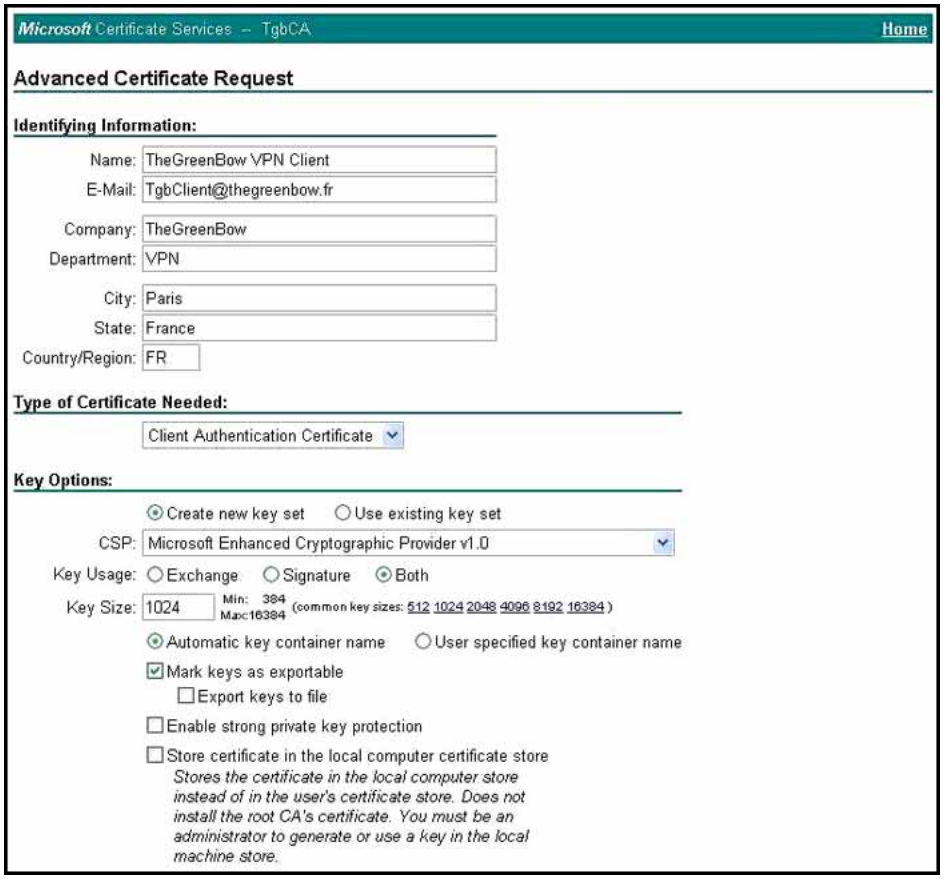


Figure 93.

6. Still on the Advanced Certificate Request screen, configure the additional options, for example, by selecting the **CMC** radio button and **SHA-1** from the Hash Algorithm drop-down list as shown in the following figure.

Figure 94.

7. Click **Submit**.

   After processing, the Certificate Pending screen displays. Wait until your request is accepted and validated by your Microsoft certificate services administrator.

   After the request has been validated and returned to you, you can view it on the Certificate Authority screen.

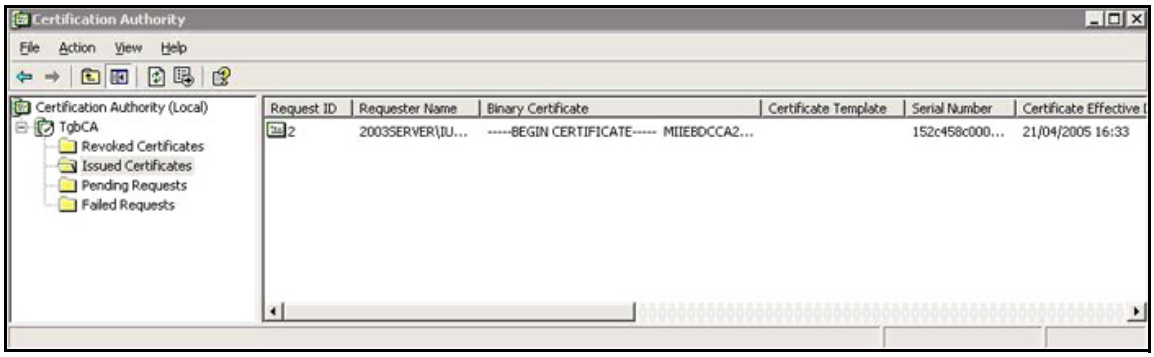


Figure 95.

8. To retrieve the certificate, return to the Microsoft Certificate Services screen, and click **View the status of a pending Certificate Request**.
9. On the View the Status of a Pending Certificate Request screen, select the certificate request that you want to view. The Certificate Issued screen displays:

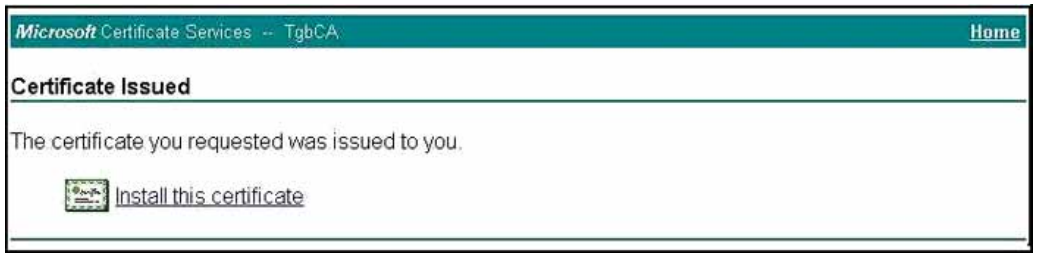


Figure 96.

10. Click **Install this certificate** to add the certificate to your local certificate store, and click **Yes** on the Root Certificate Store warning screen.

Figure 97.

11. After processing, the Certificate Installed screen displays, confirming that the certificate has been successfully installed in the Internet Explorer Certificate Store.

Figure 98.

For information about how to export a certificate from the Internet Explorer Certificate Store, see *Export Certificates* on page 150.

Sign a Certificate Request

➢ **To sign a certificate request using Microsoft Certificate Services:**

1. Connect to your certificate server (http://ServerName/CertSrv in which ServerName is the name of the CA server).
2. On the Welcome screen, select **Request a Certificate**.
3. On the Request a Certificate screen, select **Advanced Certificate Request**.
4. Select **Submit a Certificate Request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.
5. Click **Browse for a file to insert**, locate the certificate request file, and then click **Read!**. The Submit a Certificate Request or Renewal Request screen displays:

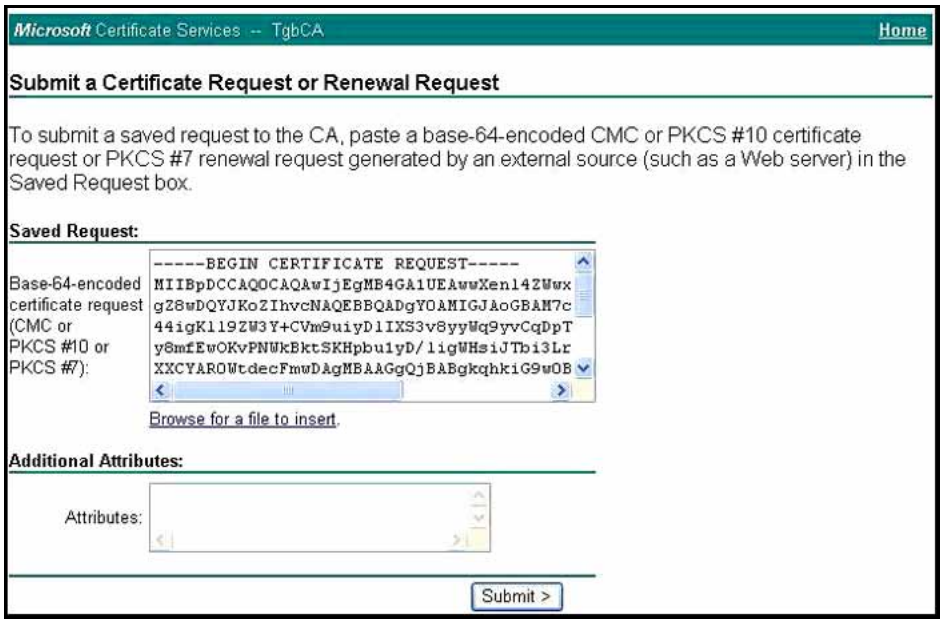


Figure 99.

6. Click **Submit**. After processing, the Certificate Pending screen displays. Wait until your request is accepted and validated by your Microsoft certificate services administrator.
7. To retrieve the certificate, return to the Microsoft Certificate Services screen, and click **View the status of a pending Certificate Request**.
8. On the View the Status of a Pending Certificate Request screen, select the certificate request that you want to view. The Certificate Issued screen displays:

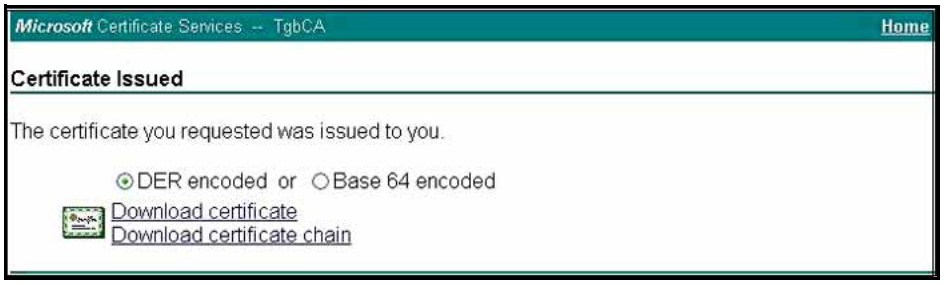


Figure 100.

9. Click **Download certificate**. A file download screen displays. Click **Save** to save the file. The default file name is certnew.cer.

Export Certificates

After a certificate has been installed in the Internet Explorer Certificate Store, you can export it in the PKCS12 file format.

➢ **To export a certificate from the Internet Explorer Certificate Store:**

1. Open Internet Explorer.

2. From the menu, select **Tools > Internet Options**.
3. Select the **Content** tab, and then click **Certificates**.
4. On the Certificates screen, click the **Personal** tab, and select the certificate that you want to export.

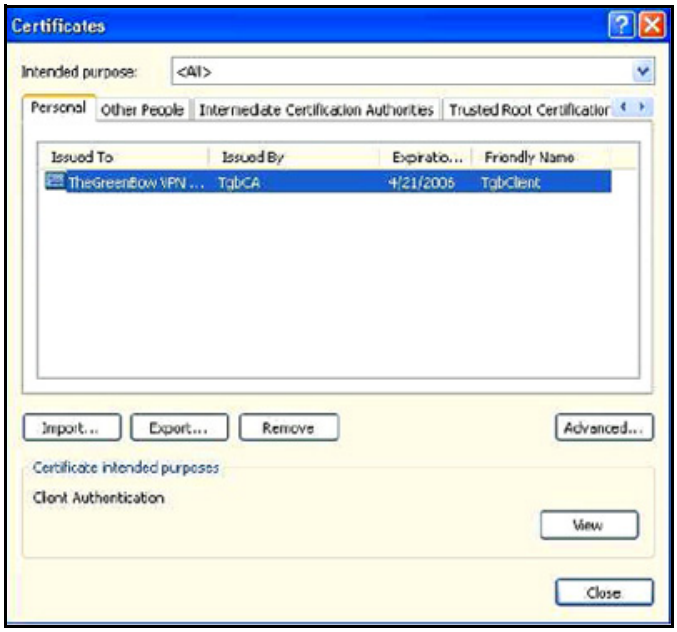


Figure 101.

5. Click **Export**. The Certificate Export Wizard displays.
6. Click **Next**.
7. Select the **Yes, export the private key** radio button.

Figure 102.

8. Click **Next**.

9. Select the **Personal Information Exchange - PKCS #12 (.PFX)** radio button and the **Include all certificates in the certification path if possible** check box. The root CA is also exported.

Figure 103.

10. Click **Next**.
11. On the Password screen, enter and confirm your password, and then click **Next**.
12. On the File to Export screen, specify the destination file path, and then click **Next**.
13. On the Completing the Certificate Export Wizard screen, click **Finish**.

OpenSSL

OpenSSL is a free noncommercial toolkit that provides a wide range of cryptographic operations. It also includes utilities for certificate management. You can find information about building and using OpenSSL at *http://www.openssl.org*.

The OpenSSL program is a command-line tool. You can download several batch scripts for certificate generation and management by downloading the TgbSmallPKI.zip file at *http://www.thegreenbow.fr/bin/tgbvpn_smallpki.zip*. Unzip this file, for example, to the root of your hard drive. After unzipping, the TgbSmallPKI folder contains the following batch scripts a Bin folder, and readme text file:

- **RootCA.bat**. Generates a self-signed root certificate.
- **UserCA.bat**. Generates a user certificate signed by the root certificate.
- **Pkcs12.bat**. Converts a P12 file into PEM files.
- **CAinfo.bat**. Displays PEM certificate information.
- **CAsign.bat**. Signs a certificate request.

- The \Bin folder contains:
  - **openssl.cnf**. A large part of the information that is included in a certificate depends on the contents of this configuration file. This file is divided into sections to help you to make the configuration more modular. You can customize this file depending on your needs. For more information, see the OpenSSL documentation at *http://www.openssl.org*.
  - **openssl.exe**, **libeay32.dll**, and **ssleay32.dll** make up the core toolkit for Windows platforms.
- **ReadME.txt**. A documentation file.

Generate a Certificate with OpenSSL

This section explains how to generate a self-signed root certificate and user certificate, and how to sign a certificate request using OpenSSL for Windows.

Generate a Self-Signed Certificate

A self-signed certificate is a certificate that is not signed by a recognized certificate authority (CA). You can use a self-signed certificate to function as a CA that issues, renews, and revokes certificates.

➢ **To create a self-signed certificate:**

Run the RootCA.bat batch script.

The following is a sample output:

```
*
! Creating Root CA folders
*
Root CA folder set to .\RootCA
Root CA key length is 1024 bits
Root CA validity is 3650 days
The system cannot find the file specified.
*
! Creating CA private key (1024 bits, 3650 days)
*
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.........++++++++++++
e is 65537 (0x10001)
*
! CA autosigning (1024 bits, 3650 days)
*
Using configuration from .\Bin\openssl.cnf
You are about to be asked to enter information
that will be incorporated into your Certificate Request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:FR
State or Province Name (full name) [France]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [TheGreenBow]:TheGreenBow
Organizational Unit Name (eg, section) []:Authority Certificate
Common Name (eg, YOUR name) []:TheGreenBow CA
Email Address []:TgbCA@thegreenbow.fr
Please enter the following 'extra' attributes
to be sent with your Certificate Request
A challenge password []:capassword
An optional company name []:TheGreenBow
Loading 'screen' into random state - done
Signature ok
subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=Authority Certificate/CN=
TheGreenBow CA/Email=TgbCA
@thegreenbow.fr
Getting Private key
"--------------------------"
"--------------------------"
Root Certificate at .\RootCA\RootCA.pem
Root Private Key at .\RootCA\CAKey.key
```

Note: The root certificate RootCA.pem and its private key CAKey.key are located in RootCA folder.

Generate a User Certificate

When you select X509 certificate authentication (that is, you select the **Certificate** radio button) on the Authentication pane of Configuration Panel screen (see *Configure Authentication* on page 45), a user certificate is used to identify a VPN IPSec endpoint and to perform signature verification operations.

The UserCA.bat batch script generates a user certificate, its private key, and a PKCS12 file. It requires an intermediate folder as a parameter. You can use this script to generate a certificate for any VPN IPSec endpoint.

➢ **To generate all required files for the VPN Client:**

Run the UserCA.bat batch script by entering **`UserCA TgbClient`**.

The following is a sample output:

```
*
! Creating User CA folder
*
Creating User Certificate folder at .\TgbClient
User CA key length is 1024 bits
```

```
User CA validity is 3650 days
*
! Creating User CA private key (1024 bits)
*
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.......++++++
..................++++++
e is 65537 (0x10001)
*
! Signing User CA
*
Using configuration from .\Bin\openssl.cnf
You are about to be asked to enter information that will be
incorporated into your Certificate Request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:FR
State or Province Name (full name) [France]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [TheGreenBow]:TheGreenBow
Organizational Unit Name (eg, section) []:VPN
Common Name (eg, YOUR name) []:TheGreenBow VPN Client
Email Address []:TgbClient@thegreenbow.fr
Please enter the following 'extra' attributes
to be sent with your Certificate Request
A challenge password []:tgbcapwd
An optional company name []:TheGreenBow
Loading 'screen' into random state - done
Signature ok
subject=/C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr
Getting CA Private Key
*
! User CA in P12 Format
*
Loading 'screen' into random state - done
Enter Export Password:
Verifying password - Enter Export Password:
TgbClient.p12 created in .\TgbClient.p12
"---------------------------"
"---------------------------"
User Certificate at .\TgbClient\TgbClient.pem
User Private Key at .\TgbClient\local.key
User Certificate Subject is:
subject= /C=FR/ST=France/L=Paris/O=TheGreenBow/OU=VPN/CN=TheGreenBow VPN
Client/Email=TgbClient@thegreenbow.fr
```

After you have run the script, the following files are the most important ones in the TgbClient folder:

- **TgbClient.pem**. The user certificate.
- **Local.key**. The private key of the user certificate.
- **Subject.txt**. The subject of the user certificate.
- **TgbClient.p12**. A file in the PKCS12 format that contains the user and root certificates, and the private key of the user certificate.

Displaying Certificate Information Using TgbSmallPKI Tools

This section explains how to display certificate information and how to extract certificates and private keys from a file in PKCS12 file by using the following batch script files:

- **Pkcs12.bat**. Converts a P12 file into PEM files.
- **CAinfo.bat**. Displays PEM certificate information.

Displaying certificate information can be useful for retrieving information from several fields such as the Issuer, the Validity date, and the Subject fields.

The CAinfo.bat batch script displays the user certificate information. It requires a certificate file as a parameter.

➢ **To display more information about the TgbClient.pem file:**

Run the CAinfo.bat batch script by entering **`CAinfo TgbClient\TgbClient.pem`**.

> ***Note:*** *The TgbClient.pem file is the user certificate that was created in* *Generate a User Certificate with Microsoft Certificate Services on page 147.*

The following is a sample output:

```
*
! Certificate TgbClient\TgbClient.pem information
*
Certificate:
  Data:
  Version: 1 (0x0)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=Authority Certificate,
CN=TheGreenBow CA
/Email=TgbCA@thegreenbow.fr
    Validity
      Not Before: Apr 19 12:44:03 2005 GMT
      Not After: Apr 17 12:44:03 2015 GMT
    Subject: C=FR, ST=France, L=Paris, O=TheGreenBow, OU=VPN, CN=TheGreenBow
VPN Client/Email=TgbClient@thegreenbow.fr
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
```

```
        RSA Public Key: (1024 bit)
          Modulus (1024 bit):
            00:ac:00:2c:1b:82:6d:32:2e:17:09:9f:13:8d:b9:
            9f:9b:db:d7:3f:f7:45:9b:f2:73:6d:8b:3d:9b:b1:
            14:99:25:22:fb:a8:56:30:9d:68:43:e9:14:84:6f:
            4c:24:fa:e2:36:84:56:2d:b2:5c:11:fd:be:b9:9e:
            ed:49:c8:c1:08:29:d0:17:ca:b8:12:41:41:55:4d:
            48:01:57:bc:22:9a:c9:48:ca:e2:c2:59:2c:78:8d:
            6d:cc:89:09:3a:97:f5:f4:b7:96:ea:da:82:0e:8c:
            87:49:a7:45:a4:74:45:31:8e:ac:be:9a:a2:8c:a1:
            16:be:f7:46:4a:94:78:31:73
          Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
      b2:ba:7c:92:9c:eb:59:c2:7e:d9:95:af:71:8b:06:2f:b8:44:
      b3:b5:2a:b7:98:0b:1e:08:97:85:c7:bc:21:1c:cf:df:15:97:
      d9:4f:e5:ec:31:14:6f:9e:b1:8a:47:37:ad:6b:4b:c8:15:bf:
      cd:8a:1b:ed:a5:f7:3e:ac:72:73:b9:bc:f6:22:b3:05:f5:26:
      40:dd:f8:4c:83:3f:25:da:68:32:8b:bd:1b:68:24:e8:df:31:
      83:5b:74:91:10:1f:6a:d0:b9:3c:f3:04:50:4c:6e:ce:c9:de:
      3a:38:fe:2d:ad:6c:6b:e6:74:38:51:0c:5b:c5:bb:6b:05:25:
      44:d9
```

References and Useful Websites

C

These references and websites are for the ProSafe VPN Client Professional / Lite that is powered by TheGreenBow.

> ***Note:*** For documentation about the *legacy* ProSafe VPN Client that is powered by SafeNet, see the following NETGEAR knowledge base links.
> *http://kb.netgear.com/app/products/model/a_id/2543*
> *http://kb.netgear.com/app/products/model/a_id/2544*

- Access to VPNG01L product information and a 30-day trial software version:

  http://kb.netgear.com/app/products/model/a_id/14552
- Access to VPNG05L product information and a 30-day trial software version:

  http://kb.netgear.com/app/products/model/a_id/14554
- VPNG01L/VPNG05L FAQs:

  http://kb.netgear.com/app/answers/detail/a_id/14903
- TheGreenBow IPSec VPN Client:

  http://www.thegreenbow.com/vpn.html
- TheGreenBow VPN documentation and manuals:

  http://www.thegreenbow.com/vpn_doc.html
- TheGreenBow VPN documentation for various VPN gateways:

  http://www.thegreenbow.com/vpn_gateway.html

  The documents that you can access from this link are based on TheGreenBow VPN Client. The NETGEAR ProSafe VPN Client Professional / Lite is powered by TheGreenBow, so configuration is likely identical or very similar.

Index

Numerics

3G interface 29

A

access control 27, 83, 130, 136
activation and Activation Wizard, software 15
activation confirmation, email address 16, 85, 136
`activmail` command, software setup 85, 136
`add` CLI command 78, 89, 140
adding, imported VPN configuration 76
address type, remote endpoint
  authentication (phase 1) 50
  IPSec configuration (phase 2) 54
AES 128, 192, and 256
  IKE, authentication (phase 1) 47
  ESP, IPSec configuration (phase 2) 54
aggressive mode 49
algorithms
  IKE, authentication (phase 1) 47
  ESP, IPSec configuration (phase 2) 54
  supported 8
alternate
  gateway 49
  server 57
Answer to Reset (ATR) codes 89
assigning certificates 67
authentication (phase 1)
  configuring 45
  no response, common problems 120
authentication algorithm
  IKE, authentication (phase 1) 47
  ESP, IPSec configuration (phase 2) 55
`autoactiv` command, software setup 85, 136
autorun.inf file 127

B

bat, file extension 128, 152
batch scripts
  for OpenSSL 152
  software setup from 128

C

CD-ROM, software setup from 127
certificate authority (CA) 68, 143, 153
Certificate Export Wizard 69
Certificate Management tool, Windows 75
certificate signing request (CSR) 149
certificates
  IE Certificate Store, exporting from 150
  importing 69
  managing 66
  OpenSSL, generating with 153
  selecting 47
  signing a request 149
  USB tokens and smart cards, using from 73
  VPN configuration file, using from 68
clearing logs 33
`close` CLI command 133, 140
command reference
  CLI commands 139
  software setup commands 135
command-line interface (CLI) commands 139
Config Mode. *See* Mode Config.
Configuration Panel screen, description 25, 41
Configuration Wizard 41
connection modes, supported 8
Connection Panel screen, description 24, 39
console shows only SEND and RECV, common problems 121
console, viewing VPN logs 33
controlling access 27, 83, 130, 136
Ctrl + Enter, Ctrl + D, Ctrl + S, shortcuts 24

D

`D` switch, software setup 85, 135
deactivation, software license 15
Dead Peer Detection (DPD) 61
delay between retries, DPD 61
DES and 3DES
  IKE, authentication (phase 1) 47
  ESP, IPSec configuration (phase 2) 54
Diffie-Hellman key length
  IKE, authentication (phase 1) 47

ESP, IPSec configuration (phase 2) 55
DNS server 57
documentation, references 158

E

email address
confirming activation 16, 85, 136
suppressing 16
embedding, VPN configurations 82, 132
Encapsulating Security Payload (ESP), settings 54
encryption algorithms
IKE, authentication (phase 1) 47
ESP, IPSec configuration (phase 2) 54
supported 8
errors 117
ESP (Encapsulating Security Payload), settings 54
evaluation, software 13
expiration, trial software license 13
`export` CLI command 89, 140
`exportonce` CLI command 89, 140
extended authentication (XAUTH) 49, 51–52
extensions, files
.bat 128, 152
.ini 89
.p12 and .pfx 72
.tgb 25, 77, 82

F

features, VPN Client 8
file extensions
.bat 128, 152
.ini 89
.p12 and .pfx 72
.tgb 25, 77, 82
firewall rules, Windows 13
firmware. *See* software. 19
FreeS/WAN 7
fully qualified domain name (FQDN) 50

G

Gina mode 57
global parameters 60
graphical user interface (GUI)
configuring appearance 83, 130, 136
description 21
GreenBow, company 158
`guidefs` command, software setup 83, 136

H

hiding
email address 16
password 64
screens and menu items 27, 83, 130, 136
Trial screen 86, 138
hybrid authentication mode 50

I

icons
desktop shortcut 35
software setup from 128
system tray 22
`import` CLI command 88, 141
`importonce` CLI command 89, 141
ini, file extension 89
installation options, software 12
installation path 85, 135
installation, silent 85, 135
interface, IP address 46
Internet Key Exchange (IKE)
rekeying lifetimes 61
restarting 33
settings 47
UDP port 61
interval, DPD 61
INVALID COOKIE, error 117
INVALID ID INFORMATION, error 119
IP addresses
authentication (phase 1) 50
IPSec configuration (phase 2) 54
local ID (VPN Client) 50
network interface 46
remote endpoint, using the Configuration Wizard 43
remote gateway 46
remote ID (remote endpoint) 50, 54
virtual (VPN Client) 54
IPSec configuration (phase 2)
configuring 52
encapsulation modes 55
no response, common problems 121
rekeying lifetimes 61
issuer, certificates 69

K

key group
IKE, authentication (phase 1) 47
PFS, IPSec configuration (phase 2) 55
keyboard shortcuts 24

L

label
authentication (phase 1) 46
IPSec configuration (phase 2) 53
lang command, software setup 86, 137
languages
changing and editing 30
supported 8, 137
launching scripts 58
legacy ProSafe VPN Client 158
license command, software setup 85, 138
license number
changing 17
entering automatically 85, 138
entering manually 16
license, software
expiration, of trial 13
transferring 15
lifetimes, IKE and IPSec rekeying 61
Linux IPSec VPN 7
Lite, VPN Client, features supported 10
local ID (VPN Client ID) 50
logs
routers 123
VPN Client 33

M

main menu 26
maintenance period, software 19
MD5
IKE, authentication (phase 1) 47
ESP, IPSec configuration (phase 2) 55
menu, main 26
menuitem command, software setup 84, 138
Microsoft certificate services 143
Microsoft Internet Information Server (IIS) 143
Mode Config 48
modes, supported for connection 8
mutually exclusive CLI commands 89

N

name
authentication (phase 1) 46
IPSec configuration (phase 2) 53
NAT port, IPSec configuration (phase 2) 62
NAT Traversal (NAT-T)
mode selection 49
modes, supported 8
NETGEAR routers and appliances, using with VPN Client 91
network analysis software tool, Wireshark 116
network drive, software setup from 129
no keystate, error 118
NO PROPOSAL CHOSEN, error 119
no response to phase 1 or phase 2 request, common problems 120
noactiv command, software setup 86, 138
number, license
changing 17
entering automatically 85, 138
entering manually 16

O

open CLI command 133, 141
OpenSSL 152

P

P12 certificates, importing 71
parameters, global 60
password command, software setup 83, 139
password, protecting VPN configurations 64
path, installation 85, 135
payload encryption 55
PAYLOAD MALFORMED, error 117
PEM certificates, importing 70
Perfect Forward Secrecy (PFS) 55
Personal Certificate Store, troubleshooting 75
phase 1 (authentication)
configuring 45
no response, common problems 120
phase 2 (IPSec configuration)
configuring 52
no response, common problems 121
PIN code, USB token or smart card 74
PKCS#12 certificates, importing 71
popup screens, system tray 23
ports
4500 (NAT) 62
500 (IKE) 61
preshared key 46
primary gateway 49
private key file, PEM 71
problems, common 120
Professional, VPN Client, features supported 10
protocols, supported for tunneling 8
Public Key Infrastructure (PKI) 51
pwd CLI command 89, 142

R

`reboot` command, software setup 85, 139
rebooting automatically, using setup commands 85
received remote ID other than expected, error 118
redundant gateway 49
reference
  CLI commands 139
  software setup commands 135
remote endpoint
  address type
    authentication (phase 1) 50
    IPSec configuration (phase 2) 54
  IP addresses
    authentication (phase 1) 50
    IPSec configuration (phase 2) 54
    Configuration Wizard 43
  pinging fails 121
remote gateway, IP address 46
remote sharing 59
`replace` CLI command 89, 142
replacing, existing VPN configuration 76
restarting, IKE process 33
retransmissions, messages 61
retries, DPD 61
root certificate file, PEM 71

S

S switch, software setup 85, 135
SafeNet, company 158
sample VPN configurations
  routers
    configuration manually 99
    configuring using the VPN wizard 93
  VPN Client
    configuring manually 108
    configuring using the Configuration Wizard 103
scripts
  opening and closing tunnels, using CLI commands 133
  specifying, using Scripts pane 57
setup commands 135
setup.exe file 82, 126
SHA-1 and SHA-256
  IKE, authentication (phase 1) 47
  ESP, IPSec configuration (phase 2) 55
sharing, remotely 59
shortcuts, keyboard 24
silent installation, software setup 85, 126, 135
smart cards
  containing certificates 68
  importing certificates from 73
  troubleshooting 74
software
  activation and Activation Wizard 15
  evaluation 13
  installation options 12
  license, deactivation and transfer 15
  maintenance period 19
  trial and trial license expiration 13
  troubleshooting activation 17
  uninstallation 20
  upgrading 19, 130
  VPN Client version 19, 26
software setup commands 135
software setup file 82
split tunneling 62
`start` command, software setup 85, 139
startup modes 29
status bar 26
`stop` CLI command 88, 142
StrongS/WAN 7
suppressing
  email address 16
  password 64
  screens and menu items 27, 83, 130, 136
  Trial screen 86, 138
system tray icon 22
system tray menu
  configuring appearance 84, 130, 138
  description 22

T

technical support 2
tgb, file extension 25, 77, 82
TheGreenBow, company 158
timeout, XAUTH 61
token codes and names, vpnconf.ini file 90
trace logs 33
trademarks 2
traffic detection, tunnel opening on 57
transferring, software license 15
translation, modifying 31
transport mode, IPSec configuration (phase 2) 55
Trial screen suppression 86, 138
trial software and license expiration 13
troubleshooting
  common problems 120
  errors 117
  Personal Certificate Store 75
  software activation 17
  USB tokens and smart cards 74

tunnel mode, IPSec configuration (phase 2) 55
tunneling protocols, supported 8

U

UDP port, IKE 61
uninstallation, software 20
unstable interface 29
upgrading, software 19, 130
USB drive
  VPN configuration, enabling 62
  VPN tunnels, opening automatically 65, 66
USB Mode Wizard 63
USB tokens
  containing certificates 68
  importing certificates from 73
  troubleshooting 74
user authentication methods, supported 9
user certificate file, PEM 71
user certificate, generating with Microsoft certificate services 147
user interface
  configuring appearance 83, 130, 136
  description 21
user private key file, PEM 71

V

versions
  VPN Client software 19, 26
  Windows 8
viewing
  certificates 68
  logs, routers 123
  logs, VPN Client 33
  VPN tunnels 39
virtual IP address 54
Vista Credential Providers 57
VPN configuration file, containing certificates 68
VPN Configuration Wizard 41
VPN configurations
  applying 25
  embedding 82, 132
  importing 35
  limiting to USB drive or computer 64
  managing 76
  protecting, with password 64
  rules for importing 78
  samples, router
    configuring manually 99
    configuring using the VPN wizard 93
  samples, VPN Client
    configuring manually 108
    configuring using the Configuration Wizard 103
  USB drive, enabling 62
VPN console, viewing 33
VPN tunnels
  common problems 121
  creating manually 44
  creating with the wizard 41
  exporting 78
  opening
    after Windows logon, using setup commands 85, 139
    automatically 56
    automatically with USB drive 65, 66
    before Windows logon 37
    manually 34
    using system tray 22
    using the Connection Panel screen 40
  using scripts to open and close 133
  viewing 39
vpnconf.ini file 90
VPNG01L and VPNG05L product information 158

W

websites, useful 158
Wi-Fi interface 29
Windows
  firewall rules 13
  supported versions 8
Windows logon, opening tunnels
  after logon, using setup commands 85, 139
  before logon 37
Windows Personal Certificate Store, containing certificates 68
WINS server 57
Wireshark, network analysis software tool 116
wizards
  certificate export 69
  overview 32
  software activation 15
  USB mode 63
  VPN configuration 41

X

X509 certificates 47, 154
XAUTH (extended authentication) 49, 51–52